**Grinding privacy in the Internet of Bodies. An empirical qualitative research on dating mobile applications for men who have sex with men**

Guido Noto La Diega[[1]](#footnote-1)\*

**Abstract**

The ‘Internet of Bodies’ (IoB) is the latest development of the Internet of Things. It encompasses a variety of phenomena, from implanted smart devices to the informal regulation of body norms in online communities. This chapter presents the results of an empirical qualitative research on dating mobile applications for men who have sex with men (‘MSM apps’). The pair IoB-privacy is analysed through two interwoven perspectives: the intermediary liability of the MSM app providers and the responsibility for discriminatory practices against the users’ physical appearance (aesthetic discrimination). On the one hand, privacy constitutes the justification of the immunities from intermediary liability (so-called safe harbours). Indeed, it is believed that if online intermediaries were requested to play an active role, e.g. by policing their platforms to prevent their users from carrying out illegal activities, this would infringe the users’ privacy. This chapter calls into question this justification. On the other hand, in an age of ubiquitous surveillance, one may think that the body is the only place where the right to be left alone can be effective. This chapter contests this view by showing that the users’ bodies are no longer the sanctuary of privacy. Bodies are observed, measured, and sometimes change as a result of the online experience. This research adopted an empirical qualitative multi-layered methodology which included a focus group, structured interviews, an online survey, and the text analysis of the Terms of Service, privacy policies and guidelines of a number of MSM apps.

**Keywords**: dating apps, men who have sex with men, privacy, intermediary liability, online discrimination, body image, online platforms

*Beare part with me most straight and pleasant Tree,*  
*And imitate the Torments of my smart*  
*Which cruell Love doth send into my heart,*  
*Keepe in thy skin this testament of me:*

*Which Love ingraven hath with miserie,*  
*Cutting with griefe the unresisting part,*  
*Which would with pleasure soone have learnd loves art,*  
*But wounds still curelesse, must my rulers bee.*

*Thy sap doth weepingly bewray thy paine,*  
*My heart-blood drops with stormes it doth sustaine,*  
*Love sencelesse, neither good nor mercy knowes*  
*Pitiles I doe wound thee, while that I*  
*Unpitied, and unthought on, wounded crie:*  
*Then out-live me, and testifie my woes.*

Lady Mary Wroth, *The Countess of Montgomeries Urania* (1621)

1. **iNTRODUCTION**

This chapter presents the results of an empirical qualitative research on dating mobile apps[[2]](#footnote-2) for men who have sex[[3]](#footnote-3) with men (‘MSM apps’).[[4]](#footnote-4) The main findings regard privacy as the common denominator of the intermediary liability of the MSM app providers and their responsibility in discriminatory behaviours against the users’ physical appearance (aesthetic discrimination). On the one hand, privacy constitutes the justification of the immunities from intermediary liability (so-called safe harbours).[[5]](#footnote-5) Indeed, it is believed that if online intermediaries were requested to play an active role, e.g. by policing their platforms to prevent their users from carrying out illegal activities, this would infringe the users’ privacy.[[6]](#footnote-6) This chapter calls into question this justification. On the other hand, in an age of ubiquitous surveillance, one would think that the body is the only place where the right to be left alone can be effective. This chapter contests this view by showing that the users’ bodies and their perceptions are no longer the sanctuary of privacy. Bodies are observed, measured and, more importantly, change as a result of the online experience.

* 1. **The Internet of bodies**

This research sheds light on a broader phenomenon, that is the Internet of Bodies (IoB),[[7]](#footnote-7) the newest phase of the Internet of Things. It may be natural to think that personal data is that data that we provide (e.g. when creating a Facebook account) or that third parties can otherwise infer from our behaviour (e.g. Google’s targeted advertising).[[8]](#footnote-8) One may be surprised, however, to discover that our body is becoming one of the most important sources of personal data. Facial recognition is the obvious example, with the iPhone X set to make it ubiquitous.[[9]](#footnote-9) One may, then, realise that with the Internet of Things our body is increasingly monitored and treated by smart devices (mainly wearables and implantables).[[10]](#footnote-10) Lastly, with artificial enhancement one is witnessing the seamless development from human beings into cyborgs (so-called cyborgisation).[[11]](#footnote-11) These are only some examples of the privacy issues in the IoB, the pair body / privacy gives rise to a number of privacy issues[[12]](#footnote-12) and much research is needed to give ‘form to the amorphous by joining it to the inchoate.’[[13]](#footnote-13)

What one would have not expected until recent times is that artificial intelligence may enable researchers to extract personal data from one’s appearance. A first, ethically questionable, step was made by those scholars[[14]](#footnote-14) who used supervised machine learning to infer criminal tendencies from the facial traits, thus allegedly showing that ‘criminals have a significantly higher degree of dissimilarity in facial appearance than *normal* (*sic!*)population.’[[15]](#footnote-15) This kind of research may resemble Cesare Lombroso’s theories[[16]](#footnote-16) whereby ‘criminals were inherently and physically different from others.’[[17]](#footnote-17) Suffice to say that those theories were greatly valued during Mussolini’s fascist administration.[[18]](#footnote-18) Taking a Law & Literature approach, then, one may think of *Minority Report*’s*[[19]](#footnote-19)* mutants whose clairvoyance powers allowed the Precrime Division to arrest suspects before they committed any crime.

More recently, it has been claimed[[20]](#footnote-20) that, thanks to deep neural networks, it is possible to identify the sexual orientation just by analysing one’s traits. According to those authors, if one has small jaw and chin, slim eyebrows, long nose, and large foreheads, one is likely to be a homosexual man, while the opposite would apply to homosexual women (bigger jaws, thicker eyebrows, etc.).[[21]](#footnote-21) Even leaving aside accuracy issues, it is not clear how this research copes, if at all, with ethnic minorities. A late Nineteenth Century precedent of this approach is constituted by Havelock Ellis’[[22]](#footnote-22) effort to position the ‘homosexual’ body as visually distinguishable from the ‘normal’ body through anatomical markers.[[23]](#footnote-23) One can only imagine how these technologies could be used in any of the fifteen countries were homosexuality is still punished with the death penalty.[[24]](#footnote-24)

In the IoB, the online presence of the bodies is changing the Internet. However, the opposite applies as well. For instance, recently, researchers[[25]](#footnote-25) have shown that looking at photos of underweight women affects the viewer’s mind in fifteen minutes. In the IoB, the Internet changes the bodies and their perception.

This research focuses on two aspects of the IoB. First, how the body and beauty ideals are affected by online dating platforms. Second, to what extent the privacy and freedom of expression of the users of these platforms is violated by the latter’s behaviour. This topic is interwoven with the one of the intermediary liability, since the traditional justification for the immunities and the absence of a general monitoring obligation revolves around privacy and freedom of expression.

* 1. **Relevance and contribution to knowledge**

Location-based (or geo-networking) dating apps are an increasingly important part of the IoB and of the Internet of Things; they are, indeed, ‘a form of ubiquitous computing.’[[26]](#footnote-26) The choice of dating apps over other mobile apps is justified because they ‘encourage the sharing of more personal information than conventional social media apps, including continuous location data.’[[27]](#footnote-27) The case study presented in this chapter regards MSM apps, because they constitute the ideal leans through which to look at privacy as both the justification for the immunities from intermediary liability, as well as bodily privacy. As to the first point, there are some high profile cases regarding the intermediary liability of MSM apps.[[28]](#footnote-28) As to the second one, while the body and its perception are at the centre of the mating ritual in general,[[29]](#footnote-29) this seems particularly true for most MSMs.[[30]](#footnote-30) Indeed, it has been noted that the ‘body image issues of gay men are wildly out of control.’[[31]](#footnote-31) Many MSMs believe they do not deserve a relationship because their body is not attractive enough; it would seem that it is ‘all about the body.’[[32]](#footnote-32) Scholars have consistently found that there is ‘greater appearance potency in the gay subculture.’[[33]](#footnote-33) This research leaves out lesbian users because it has been proved that the physical appearance plays a key role in men’s dating, less so in women’s one.[[34]](#footnote-34) Finally, the choice of this case is justified not only by the importance of the body within the MSM community, but also by the role of dating apps in the said community. Indeed, most same-sex couples met online,[[35]](#footnote-35) and ‘(t)he most striking difference between the way same-sex couples meet and the way heterosexual couples meet is the dominance of the Internet among same-sex couples.’[[36]](#footnote-36)[[37]](#footnote-37) The online dating market is growing, generating revenues for US$1,383m in 2018[[38]](#footnote-38). In the US, which is the main market,[[39]](#footnote-39) the only MSM app in the top 10 is Grindr (Fig. 1). The focus on this app is also explained by the fact that while Tinder and Grindr are the dating apps with more weekly active users in the world, Grindr is ranked higher than Tinder in terms of users’ engagement.[[40]](#footnote-40) Additionally, it has been recently uncovered that Grindr shares HIV status data and sexual preferences data with third parties,[[41]](#footnote-41) which raised the question to what extent can long and illegible Terms of Service, privacy policies, guidelines, etc. (collectively ‘legals’) justify such practices, especially now that the General Data Protection Regulation (GDPR)[[42]](#footnote-42) is in force.

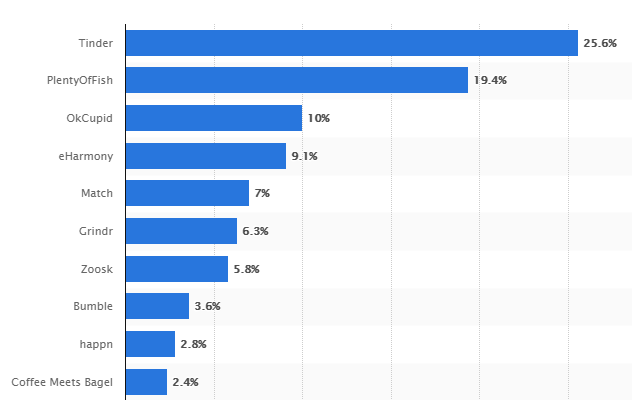


Fig. 1. Online dating market share in the US[[43]](#footnote-43)

This work contributes to the advancement of existing literature in a twofold way. First, by assessing the privacy implications of location-based online services beyond the location data[[44]](#footnote-44) or the cross-border issues.[[45]](#footnote-45) Second, more generally socio-legal research on MSM apps is still in its infancy,[[46]](#footnote-46) and the findings regarding traditional dating sites do not necessarily apply to mobile apps, which privilege picture-based selection, minimise room for textual self-description, and draw upon existing Facebook profile data.[[47]](#footnote-47) Even though some scholars[[48]](#footnote-48) are carying out socio-legal research on MSM apps, no academic research has ever explored privacy and intermediary liability in MSM dating apps,[[49]](#footnote-49) not even with regards to non-MSM[[50]](#footnote-50) dating apps.[[51]](#footnote-51) Third, by reflecting on exclusionary practices that go beyond the traditional categories taken into account by discrimination laws.

**1.3 Research methods**

The chapter adopts a multi-layered empirical qualitative methodology. The first layer was a study of privacy, intermediary liability, and discrimination laws in the EU, seen from the perspective of the UK implementations. Second, a focus group was organised with users of MSM apps to understand what are the main issues they encountered during the online dating experience, with particular regard to privacy, intermediary liability, and aesthetic discrimination. Third, text analysis was conducted with regards to the legals of fourteen apps (47 documents). Alongside a content analysis, this chapter measured the readability of the legals of Grindr, PlanetRomeo and Hornet using the tests performed by the software Readable.io, *i.e.* the Flesch-Kincaid Grade Level, the Flesch-Kincaid Reading Ease, the Gunning-Fog Score, the Coleman-Liau Index, the SMOG Index, the Automated Readability test, the Spache Score, and the New Dale-Chall Score.[[52]](#footnote-52) The purpose of this phase was to assess whether the practices lamented by the participants to the focus group as a contractual basis and whether the legals were enforceable in light of their readability and content. The fourth methodological layer was an online survey (hereinafter the ‘MSM survey’) distributed over a semester[[53]](#footnote-53) to 54 users of MSM apps recruited passively[[54]](#footnote-54) via an ad-hoc account active on Grindr,[[55]](#footnote-55) PlanetRomeo, Hornet, and Scruff.[[56]](#footnote-56) The questionnaire had 17 questions about three main points, i.e. the users’ expectations about privacy and liability of platforms, users’ attitude towards and experience of the legals, and their aesthetic discrimination experiences. Lastly, structured interviews were carried out with spokespeople of two MSM app providers. This had a twofold function. First, to collect data on practices which are not documented in the ‘legals’, e.g. in terms of take-down policies. Second, to inform the MSM app providers of the users’ concerns in order to raise awareness and in the attempt of having these providers adopt fairer policies.

The sample and the research are not and do not aim to be representative of the whole MSM population. Unlike quantitative research, qualitative methods do not aim to be representative of the entire relevant population, nor to present results that could be universally generalised.[[57]](#footnote-57) Therefore, despite the sample not being representative, the findings are worth of presentation because clear trends have been emerging during the collection and analysis of the data. Future research should attempt to broaden the sample by using a larger number of apps to recruit participants and by changing the location from where these are accessed. It may also be explored the possibility of a comparison between MSM apps and non-MSM apps. Qualitative methods focus on saturation, as in obtaining a comprehensive understanding by continuing to sample until no new substantive information is acquired.[[58]](#footnote-58) In terms of sampling method, purposive sampling was chosen, a’a technique widely used in qualitative research for the identification and selection of information-rich cases for the most effective use of limited resources.’[[59]](#footnote-59)

**2. The Internet entering the body. aesthetic discrimination.**

Traditionally, the body and the home are the main examples of private ‘places’ where people are entitled to their privacy. The body is seen as a place of privacy, for instance in those countries where nudity is restricted to private environments or that security checks cannot be overly invasive.[[60]](#footnote-60) It has been underlined, moreover, that many aspects of the body are privacy-sensitive, though there are significant changes depending on the cultural context (eg the female body in most Islamic cultures).[[61]](#footnote-61) In an age of surveillance and ubiquitous computing, however, the privacy expectations are changing profoundly, to the point that people have to endure privacy invasions even in their own bodies, be it in the form of implanted smart devices or, more broadly, as an intrusion in the perception itself of one’s own body. In the IoB, the online presence of bodies is changing the Internet and, accordingly, the Internet is changing the bodies. The focus of this section is on exclusionary practices based on the physical appearance, going under the name of aesthetic discrimination.

One of the main issues emerged during this research is that MSM apps are places of exclusion base on the users’ physical appearance. Profile descriptions on MSM apps are significantly characterised by the exclusion of entire segments of population based on their race and appearance (see Fig. 1).[[62]](#footnote-62) It is, therefore, questionable why whereas racist profile descriptions on dating apps are considered unacceptable (and rightly so), ‘using an automatic ‘filter’ to exclude certain kinds of bodies does not.’[[63]](#footnote-63) Even more problematic than the filters, used to view only users that reflect certain characteristics (e.g. ‘twinks’), are the profile descriptions that overtly exclude users both for racist and aesthetic reasons. This research shows that these facts have important consequences in terms of body image and self-esteem. This is in line with the research on the use of nudity in advertising, which proves that ‘(s)carcely dressed models had a negative effect on individuals’ body esteem compared to dressed model.’[[64]](#footnote-64) It has been shown[[65]](#footnote-65) that there is an abundance of MSM users who rely on photos where their flesh and skin are exposed (so-called hypersexualised masculinities).[[66]](#footnote-66) Along the same lines, a study found that MSM magazines feature ‘more images of men that were appearance ideal, nude and sexualized than the straight men's magazines.’[[67]](#footnote-67) And dating has become akin to advertising; to put it in a user of MSM apps’ words ‘any dating profile sort of thing is a place for advertising, it’s selling yourself essentially, you obviously, you’re using that profile with an aim in mind, so it’s a market, it’s a meat market essentially.’[[68]](#footnote-68) In conclusion, both in dating and in advertising the common exposition of nudity produce negative effects on the body and self-esteem.[[69]](#footnote-69)

## 

Fig. 2. Screenshot of a Scruff’s user profile description.

This research started with a focus group where some users of MSM apps informed this author that these apps were making them feel as if their body were wrong. One of them, a self-perceived ‘stocky’ guy in his thirties, stated that his profile pictures were blocked because he showed his torso and tummy (see Fig. 3), but similar pictures of users whom he considered ‘fitter’ were accepted by the same apps. A virtual tour carried out by this author on Grindr seemed to confirm that the fit shirtless torsos constituted a significant number of the profile pictures displayed (see Fig. 4).[[70]](#footnote-70) One of the aspects that this research aimed at finding out was whether the participants to the focus group had been merely unlucky or whether these apps were actually discriminating against users with a certain kind of body.



Fig. 3. Profile picture rejected by Grindr for alleged breach of the Profile Guidelines

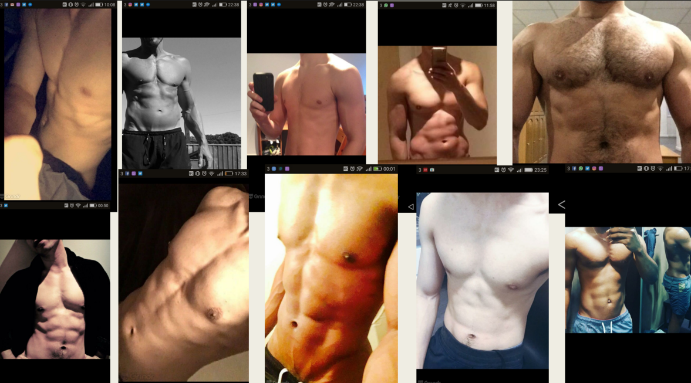


Fig. 4. Profile pictures of Grindr’s users.

As to the other participants to the focus group, who stated not to feel at ease with their own body as a consequence of the use of MSM apps,[[71]](#footnote-71) this work endeavoured to resolve a dilemma. In simple terms, do MSM exclude interactions with users whose body is not fit, young, white, (at least seemingly) abled, and masculine because they are naturally inclined to do so or the apps play a role in creating or at least reinforcing a specific type of body which is deemed acceptable and sexually desirable, whilst excluding those who do not conform to the proposed model? Recently, research confirmed that ‘exclusion is found in the way users celebrate and reinforce ideas of traditional masculinity and denigrate and reinforce stereotypic ideas about femininity embodied by some gay men.’[[72]](#footnote-72) Whilst treating a person differently on the basis of the colour of the skin is the paradigm of discrimination (and, therefore, discrimination laws may provide some protection to users belonging to ethnic minorities), no such thing is accepted with regards to the ‘aesthetic discrimination’, that is the unfavourable treatment based on a person’s appearance. There is a growing discussion about phenomena such as body shaming,[[73]](#footnote-73) fat shaming / fattism,[[74]](#footnote-74) ageism,[[75]](#footnote-75) internalised homophobia[[76]](#footnote-76) (that usually victimises camp or feminine guys), and ableism.[[77]](#footnote-77) However, they are treated as something radically and ontologically different to racial discrimination. An analysis of the responses to the MSM survey made clear, however, that users do not perceive racial discrimination and aesthetic one as intrinsically different things. This chapter argues that, even though aesthetic discrimination and the racial one have differences, they overlap and are closely related, because they are not a matter of mere taste:[[78]](#footnote-78) in excluding certain bodies, one is embodying and expressing heteronormative and capitalist values and power dynamics.[[79]](#footnote-79) Heteronormative because it ‘is through the overwhelming and felicitous norms of heterosexuality that queers understand and resignify desire.’[[80]](#footnote-80) This confirms the findings[[81]](#footnote-81) according to which the present heteronormative cultural and legal framework reflects a focus upon the ‘good gay’ as opposed to the ‘bad queer.’[[82]](#footnote-82) ‘Capitalist’ because the data collected suggests that the ‘acceptable’ MSM is a highly productive and respectable member of his community who embraces and even exacerbates the male / female binary.[[83]](#footnote-83) Similarly, it has been noted that ‘gay men’s place within the hierarchy of society is below that of heterosexual males and those presenting traditional masculinities, and thus social-dominance orientation can be attributed with a preference of men presenting as masculine over those with queer masculinities.’[[84]](#footnote-84) Along the same lines, one can observe that ‘(f)ar from being spaces of experimentation, exploration, and play in regard to gender, these online collectives maintain many of the dominant and oppressive notions of how individuals should act based on their biological sex.’[[85]](#footnote-85) The erasure of bodily differences, moreover, has been read as a new form of fascism.[[86]](#footnote-86) Less critically, one may see the preference for a masculine as the confirmation of that literature[[87]](#footnote-87) according to which highly sex-typical faces are considered more attractive.

Moving on to closely analyse the MSM survey distributed by this author, of the 54 users who were surveyed, 90 per cent of the respondents were white and more than half were British. As to the sexuality, 80 per cent identified themselves as gay , 6 per cent as bisexual, 2 per cent as queer, 2 per cent as questioning, and 2 per cent as straight/gay.[[88]](#footnote-88). While nearly 90 per cent described themselves as males (or men, masculine, cisgender), only 2 per cent identified as queer.[[89]](#footnote-89) A vast majority reported experiences of direct discrimination while using MSM apps (88 per cent), but 10 per cent declared not to be discriminated against. In descending order, the reported forms of online discrimination were homophobia (28 per cent), fat shaming (20 per cent), ageism (14 per cent), generic aesthetic discrimination (12 per cent), racism (12 per cent), femme-phobia[[90]](#footnote-90) (6 per cent), internalised discrimination[[91]](#footnote-91) (6 per cent), queer-phobia[[92]](#footnote-92) (4 per cent), biphobia (2 per cent). Some other forms of discrimination, such as transphobia and ableism, were not reported probably because of the limited sample. Some of these categories overlap. For instance, femme-phobia, internalised homophobia, and queer-phobia regard by definition male individuals perceived as feminine or gender non-conforming. On this aspect, recent studies found that ‘smartphone applications for gay men are reinforcing ideas of masculinity.’[[93]](#footnote-93) This is in line with the works that observe that ‘it is through the erasure of the effeminate queer male as a desirable and desiring subject that the masculine Grindr user reveals the overwhelming anxiety linked to his sexual legibility.’[[94]](#footnote-94) The analysed phenomena do not manifest themselves only in dating platforms; indeed, it has been pointed out that misogyny and homophobia characterise most online interactions, including social networks and videogames.[[95]](#footnote-95)

Most responses show that there is a certain body which is perceived as right and one which is deemed wrong.[[96]](#footnote-96) For instance, some respondents say ‘[i]f you don't fit a mould, then don't even bother’,[[97]](#footnote-97) or ‘I don't have the right body,’[[98]](#footnote-98) and ‘I felt discriminated by other app's users for my physical aspect.’[[99]](#footnote-99) Not fitting the acceptable aesthetic model can lead to be ignored or to verbal or physical violence. In one of the responses one reads: ‘[o]ften have people call me fat, ugly, disgusting etc. I've had obscenities shouted at me on the street due to my apperences (sic).’[[100]](#footnote-100) This can have dangerous consequences. A participant was discriminated against because perceived as feminine and, therefore, he ‘stopped going out to dance for a long time, in the fear of being targeted as gay in heteronormative spaces, and as an undesirable-bodied individual in homonormative spaces.’[[101]](#footnote-101) Other respondents could not find a job because of their gender non-conforming appearance or were victims of mobbing on the workplace, particularly in traditionally male-dominated industries.[[102]](#footnote-102) Others wished to be able to afford plastic surgery and one of them expressed suicidal tendencies. This constitutes an advance in the existing literature, which has hitherto focused the effects of weight discrimination on the willingness to adopt unhealthy behaviours and eating disorders.[[103]](#footnote-103) These findings are in line with those of a recent research[[104]](#footnote-104) about Tinder, that found that the popular app’s users have low levels of satisfaction with thir faces and bodies and they have high levels of shame about their bodies. The same study found that men report lower levels of self-esteem;[[105]](#footnote-105) future research should investigate whether the level of body-related self-esteem varies according to the sexuality of the user.

Overall, the contention is that given the pervasiveness of exclusionary practices based on the physical appearance and due to their negative consequences, there are good reasons to rethink discrimination laws. If this chapter’s suggestion were accepted, this could lead to an extension of discrimination laws to encompass new protected characteristics[[106]](#footnote-106) and new scenarios.[[107]](#footnote-107) However, even in the event of a rejection of the parallel between these forms of discrimination, it is hoped that this research will shed new light on the aesthetic discrimination, with consequences at least in terms of a change in the apps’ policies and the users’ behaviour, as well as a consistent application of hate speech laws to these phenomena. This research already produced a positive impact, in that one of the platforms amended its legals after its spokesperson was interviewed by the author. Indeed, this author brought to the spokesperson’s attention that it was unacceptable to invite users to ‘take it like a man’ when another user rejected them. The day after the interview the spokesperson confirmed that ‘after our call I had that *problematic language* removed from our etiquette guide. We are in the process of *updating all the language* but I at least wanted to make sure that that part was removed.’[[108]](#footnote-108)

With the Internet entering one’s own body, the traditional assumption of the body as the paradigm of the place of the right to be left alone should be revisited.

**2.1 The responsibility for aesthetic discrimination**

While over 90 per cent of the respondents to the MSM survey feel pressured to look different from how they normally look, they are divided as to where these pressures come from. Four out of 10 users feel that MSM apps are exerting pressures to change their bodies. However, 33 per cent of the respondents blame it on society as a whole and 25 per cent on other users or the MSM community. In the latter’ view, one can hear the echo of the ‘gay clone’ theory[[109]](#footnote-109), whereby the gay culture produces its own stereotypical identity and rules of power. More recently, it has been observed that ‘men are producing their own standards of participation that exclude differences from within their own community.’[[110]](#footnote-110) While it seems true that the norms regulating the MSM online environment reproduce heteronormative dynamics and that differences tend to be erased,[[111]](#footnote-111) it is debatable that this is a case of pure autonomy in the literal sense of self-production of norms. The platforms, indeed, seem to play a critical role in setting a standard of aesthetic acceptability, e.g. with their use of muscled models in advertising, but also by allowing body-related exclusionary practices.

Prima facie, it might seem that MSM apps are not responsible for aesthetic discrimination. Some of them declare it publicly. So, for instance, Hornet ‘will never accept any rejection that refers to a person’s age, religion, race, or size.’[[112]](#footnote-112) When the issue was brought to their attention, spokespeople for two important MSM apps accept that the criticised phenomenon exists, but either they claim that it would be incorrect to label it as discrimination or that the app should not be considered responsible because ‘we are just platforms.’[[113]](#footnote-113) Some users, in turn, see the MSM apps as responsible because ‘[t]hey create the platform and create the presumption that they'll police it accordingly. Once you do that, you're responsible.’[[114]](#footnote-114)

The survey did not confirm – yet did not refute[[115]](#footnote-115) – the hypothesis put forward by one of the participants in the focus group stage*,* according to whom there would be a pattern whereby only profile pictures of fit and young bodies go through the filtering system of MSM apps. However, most respondents to the MSM survey do believe that these apps are promoting a fit, young, white, and masculine aesthetic model. This is consistent with the existing literature[[116]](#footnote-116) pointing out that the way MSM apps are designed reinforces aesthetic discrimination. For instance, by requiring (and sometimes forcing) users to fill in the information on height, weight and body type, these apps are contributing to the creation of a standard of beauty in the MSM community.[[117]](#footnote-117) More generally, another study[[118]](#footnote-118) found that 35 per cent of MSM users experience abuse and harassment online.[[119]](#footnote-119)

Many respondents infer the said promotion of an aesthetic model from the pictures used by MSM apps in advertising. They mostly show ‘fit muscly guys,’[[120]](#footnote-120) ‘fit masculine men,’[[121]](#footnote-121) etc. Some participants, however, say that these apps ‘just mirror those social norms’[[122]](#footnote-122) and even if it is true that the model proposed is that of the ‘white muscular fit men, very masculine looking,’[[123]](#footnote-123) this happens because people would not use the apps ‘if they were marketed through pictures of fat, or feminine-looking, or traditionally conceived as ‘ugly men.’’[[124]](#footnote-124) The issue is resolved by this user by saying that ‘Grindr, Romeo, and Hornet are definitely not queer activist apps. They try to sell, and masculinity and fitness are what sells.’[[125]](#footnote-125) While the depiction of dating as a market confirms previous studies,[[126]](#footnote-126) a clarification needs to be done with regards to latter response. This author does not expect profit-maximising entities to become queer advocate groups;[[127]](#footnote-127) however, it would be surprising if they did not play any role in the setting of body standards, given the importance of these apps in the everyday life of MSM.[[128]](#footnote-128) Moreover, it is not necessarily true that fit bodies sell more than average ones. It has been found[[129]](#footnote-129) that while the exposure to thin ideals harms an individual’s body esteem, it is not a more effective marketing strategy.

Along the same lines, another respondent says that the ‘discrimination comes from within the community. The only way in which MSM apps promote it is by not being vigilant enough to users who abuse it.’[[130]](#footnote-130) If the lack of vigilance were true, it may be explained with the fact that if the app provider were vigilant, it would not be able to invoke the safe harbor in the event of an intermediary liability claim. Therefore, let us look into this intricate regime.

**3. The intermediary liability of online dating platforms for men who have sex with men**

It must be said that being responsible for imposing or reinforcing a certain aesthetic model is not the same[[131]](#footnote-131) as being liable for the illegal activities carried out by the users (e.g. unauthorised use of personal data, hate speech, stalking, etc.). Liability is responsibility’s legal *species*. Privacy, however, plays an equally important role in both the scenarios, because privacy is eroded in an IoB world where one loses control over one’s body and, at the same time, privacy is invoked as a justification to the immunities from intermediary liability.[[132]](#footnote-132) ‘Intermediary liability’ refers to the liability of online intermediaries (*e.g.* a social networking website) for illegal activities carried out by third parties using the platform made available by the intermediaries themselves. Hosting providers[[133]](#footnote-133) are immune from liability if they do not have actual knowledge of the illegal activities or information and, as regards claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent.[[134]](#footnote-134) Alternatively, they can invoke the safe harbour if they act expeditiously to remove or disable access to illegal information that they store upon obtaining said knowledge or awareness.[[135]](#footnote-135) Moreover, they will be liable in damages only if there is evidence of awareness of facts or circumstances from which the illegal activity or information is apparent.[[136]](#footnote-136) The current legal framework does not provide a clear answer to a number of questions raised by user-generated content and, more generally, user behaviour. It is unclear, for instance, what happens if terrorism-related videos are shared on Facebook and the company does not promptly remove the content, lacking a proper take-down notice.

The sections above showed that MSM apps can be used for illegal activities such as hate speech as well as for discriminatory practices. This is not the only illegal use of these apps. Other examples may include the creation of fake profiles for the purposes of stalking and harassment. An example of this is provided by *Herrick v Grindr*.[[137]](#footnote-137) In February 2017, a US court found in favour of Grindr in a case where a user had been stalked and harassed by 400 men and the platform had ignored his requests to block the fake profile that invited Grindr’s users to have sexual encounters with the plaintiff[[138]](#footnote-138). The passive attitude of the app provider persisted even after the lawsuit began (Fig. 5).



Fig. 5. Tweet by the plaintiff in *Herrick v Grindr*[[139]](#footnote-139)

Another instance of illegal use of MSM apps became famous when a man stalked, drugged, raped, and killed three teenagers hooked-up on Grindr.[[140]](#footnote-140) Like other times,[[141]](#footnote-141) Grindr did not cooperate and one may imply that this is because cooperating might be seen as an admission that the platform has knowledge of the illegal activities carried out by its users or that it is in the position to stop them or prevent further consequences from happening. Consequently, in the said cases, if Grindr knew, it would have not be able to invoke the immunity from intermediary liability.[[142]](#footnote-142)

In the EU, the intermediary liability regime was harmonised by the eCommerce Directive and Brexit will not have an immediate direct impact in this field. In the UK, the main references in terms of intermiadiary liability are the eCommerce Regulations, the Defamation Act 1996,[[143]](#footnote-143) and the Defamation Act 2013.[[144]](#footnote-144) To add to the complexity, it is not clear if the common law defence of innocent dissemination survives, or if it has been replaced by the statutory defences[[145]](#footnote-145). The European and English laws on intermediary liability revolve around three safe harbours: mere conduit, caching, and hosting. However, unlike the European matrix, the English implementation does not provide for an absolute exclusion of liability. Indeed, the main difference seems to be that they do not exclude intermediaries’ liability altogether. Conversely, they allow injunctive relief, while excluding damages, any other pecuniary remedy, and criminal sanctions[[146]](#footnote-146). Another notable addition is that reg 22 presents a non-exhaustive list of factors to help courts assessing if the intermediary has actual knowledge as required by regs 18 and 19 on caching and hosting. Courts shall have regard to, inter alia, whether a service provider has received a notice through a means of contact made available in accordance with reg. 6(1)(c)[[147]](#footnote-147) and the extent to which the notice includes the full name and address of the sender of the notice, details of the location of the information in question, and details of the unlawful nature of the activity or information in question. Thus, on this point, the eCommerce Regulations provide a regime, which is even more favourable to intermediaries, if compared to the eCommerce Directive. Suffice to say that there is no sanction for an intermediary that does not provide an easy way to contact them. For instance, this author unsuccessfully tried to find a way to get in contact with one of the selected MSM apps, but it was not possible to find their email or any contact form. Therefore, it may be argued that intermediaries could shield themselves by making it difficult for users to issue a notice. This does not seem fair. More generally, the formal emphasis on the notice – as opposed to a more flexible approach where knowledge can be inferred by a number of factors – leads to abuses, such as the ones recently uncovered with regards to eBay, that removes listings against mere allegations of patent infringement, without actual proof, let alone court orders.[[148]](#footnote-148) This change of policy may be seen also as a reaction to the increased pressures on intermediaries to take a more active role in policing the Internet.[[149]](#footnote-149)

In the UK, like in the rest of Europe and in other jurisdictions, the intermediary liability regime was designed to favour intermediaries[[150]](#footnote-150) in a twofold way. First, by allowing them to escape liability when they play a merely passive role in the intermediation and/or have no knowledge of the illegal activities carried out by the third parties. Second, by pointing out that one cannot impose on them a general obligation of monitoring. Otherwise, the rationale goes, there would be a violation of fundamental rights such as privacy and freedom of expression.[[151]](#footnote-151) The leading case is ***Scarlet Extended SA v SABAM****[[152]](#footnote-152)*, which stated that the European regime of intermediary liability is rooted in the online users’ ‘right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter’ [[153]](#footnote-153) of Fundamental Rights of the EU. In the lobbying battle to secure their own immunity, Internet service providers argued that ‘nor was it desirable or possibly legal for them to (manually check all the material which passed through their servers) without invading the privacy and confidentiality of their subscribers.’[[154]](#footnote-154) Along the same lines, in September 2017 the European Commission underlined that the operation of technical systems of protection and identification of illegal content online ‘must however take place within the limits of the applicable rules of EU and national law, in particular on the protection of privacy and personal data and the prohibition on Member States to impose general monitoring obligations.’[[155]](#footnote-155) All in all, the privacy-based justification for the immunity from liability sounded spurious already at the time of the adoption of the eCommerce Directive, but now, in light of the actual practices of most online intermediaries, there is further evidence of its untenability.

Intermediaries are increasingly asked to take on a policing role through responses to legal requirements, industry self-regulation, as well as through their business practice.[[156]](#footnote-156) Concerns have been expressed that Internet service providers could be become ‘copyright cops,’ thus compressing privacy, freedom of expression and due process.[[157]](#footnote-157) Similarly, other authors[[158]](#footnote-158) affirm that the implementation of the ‘initial obligations’[[159]](#footnote-159) of the Digital Economy Act 2010[[160]](#footnote-160) would allegedly conflict with the European Convention on Human Rights.[[161]](#footnote-161) More recently, in September 2017 the European Commission presented a set of guidelines for online intermediaries ‘to step up the fight against illegal content online in cooperation with national authorities, Member States and other relevant stakeholders.’[[162]](#footnote-162) Unsurprisingly, the European trade association representing online platforms reacted with utter disappointed to the Commission’s approach to the regulation on online intermediaries.[[163]](#footnote-163) Even though this trend may lead to a further compression of the freedom of expression and of the right to privacy,[[164]](#footnote-164) it is recognised that the level and extent of intermediaries’ duties is a matter of balancing policy needs, so the regime of immunities may fluctuate.[[165]](#footnote-165) There may be good reasons for a reassessment of the balance today. Illegal activities (also beyond copyright infringement) are increasingly carried out online.[[166]](#footnote-166) Online intermediaries appear more and more powerful. Intermediaries tend not to prevent, nor react to illegal activities carried out by their users and, what is worse, this could be a reaction to the intermediary liability regime that protects them if they appear to be neutral. Additionally, this study confirms that there is a degree of hypocrisy in rooting the immunity from liability in the right to privacy, which is then clearly violated by the same intermediaries.

Coming back to the MSM survey, the respondents were asked question about intermediary liability and the role of privacy. 20 per cent of the participants believe that MSM apps should be held liable because they create the expectation of policing the platform. Those who disagree, however, point out that MSM apps should be more active in preventing and reacting to illegal activities. The passive attitude of MSM apps may be explained in light of the intermediary liability regime, because the app providers may fear that if they were proactive they could not invoke the immunity from liability analysed below[[167]](#footnote-167).

The respondent quoted above, who linked the policing of the platform to the liability is right in believing that if a platform polices the user-generated content and users’ behaviour they cannot claim immunity,[[168]](#footnote-168) but these apps deny that they have any actual control and therefore knowledge. For instance, Grindr declares that it ‘does not control the content of User Accounts and profiles.’[[169]](#footnote-169) From this supposed lack of control the app makes follow a lack of obligation to monitor users (but a right to do so) and, correspondingly, an absolute disclaimer of liability.[[170]](#footnote-170) The lack of control seems excluded by the fact, for instance, by the fact that the MSM apps access and store private messages and all the materials (including photos, location, and videos) ‘for archival purposes or as otherwise allowed by law.’[[171]](#footnote-171) These data are used *inter alia* for marketing purposes,[[172]](#footnote-172) therefore the apps should at least allow an opt-out mechanism, which is not provided.[[173]](#footnote-173) Moreover, the user-generated content is preliminarily filtered[[174]](#footnote-174) and both spokespersons confirmed that this operation is not automated. In other words, there is a team manually overviewing all user-generated content and this puts the app provider in the position to know if the platform is used for illegal purposes.[[175]](#footnote-175) Over 40 per cent of the users said their profile pictures had been rejected and their accounts had been suspended at least once. The main reason for this seemed to be suggestive photos (though this was interpreted broadly, as encompassing for instance the showing of navel hair),[[176]](#footnote-176) followed by vulgar language. This shows that MSM apps have control over their users’ activities (in defiance of the right to privacy) and, therefore, they are in the position to know if something potentially illegal happens on the platform. If this is the case, they cannot invoke the immunity from intermediary liability analysed below. One may wonder why MSM apps control (if not police) their users' activities. The answer provided by both the spokespeople interviewed was that they are required to do so by the app stores[[177]](#footnote-177) i.e. mainly by Google and Apple[[178]](#footnote-178). This trend dates back to the agreement between the Attorney-General of California (the ‘California agreement) and six app store providers;[[179]](#footnote-179) from that document stemmed the obligation for these providers to include ‘a field for privacy statements or links in the application submission/approval process for apps.’[[180]](#footnote-180) More recently, legal scholars have suggested that, since app developers and users are located around the world, thus making it difficult for privacy laws to be enforced, app stores play a ‘central role in determining the standard of data privacy which is afforded to users.’[[181]](#footnote-181) A spokesperson of an MSM app provider[[182]](#footnote-182) said that, in order to allow the app store providers to monitor the compliance with their content policies, they provide the app store providers with a username and password; Apple and Google, then login as a normal user and monitor the enforcement of their guidelines.[[183]](#footnote-183) From the data collected with the MSM survey, it seems clear that this practice is not consistent with the privacy expectations of the users. This backdoor left to app store providers may be considered in the context of the California agreement that had the purpose to rely ‘to a great extent on the store as a protector of privacy.’[[184]](#footnote-184) Reportedly,[[185]](#footnote-185) finally, the app stores would be responsible for imposing very strict terms to the MSM apps, that would be required to police the platforms in order not to be banned by the app stores. Funnily enough, however, the MSM apps’ terms are usually stricter than the app stores’ ones, with the only exclusion of discriminatory content, which is absolutely prohibited by Apple’s app store guidelines,[[186]](#footnote-186) but not from Grindr, PlanetRomeo or Hornet.[[187]](#footnote-187) The fact that MSM apps have filtering mechanisms in place, while endangering their immunity from intermediary liability, may be explained in light of the app store guidelines, which require MSM apps to have in place a method for filtering objectionable material from being posted to the app.[[188]](#footnote-188)

Now, let us assume that MSM apps do not in fact monitor or have control over their users and the content they generate. If this were the case, MSM apps should at least react promptly upon receiving a notice where the user reports some illegal activity. If the illegal content is not taken down nor its access disabled, under the intermediary liability regime the MSM app provider shall be found liable. Surprisingly, therefore, the MSM apps' legals provide that ‘under no circumstances, including negligence, will Grindr be liable (for the) interactions with Grindr or any other user (…) even if Grindr or a Grindr authorized representative has been advised of the possibility of such damages.’[[189]](#footnote-189) Or that PlanetRomeo’s ‘liability for consequential damages (…) arising out of, or in connection with the Agreement or these Terms of Use (…) independent of whether the User provides notice to (PlanetRomeo) of such potential injury, damages or loss, is excluded.’[[190]](#footnote-190) Such clauses go against the letter and purpose of the eCommerce Directive[[191]](#footnote-191) and UK Regulations[[192]](#footnote-192) whereby immunity cannot be claimed if there is knowledge of the illegal activities carried out by the platforms’ users.[[193]](#footnote-193) These clause are, therefore, unenforceable, notwithstanding the attempts of the MSM apps to make the user believe that the only remedy is to refrain from using the service.[[194]](#footnote-194)

The EU, in regulating intermediary liability, sought to strike a balance between competing interests such as reputation, freedom of speech, privacy, competitiveness.[[195]](#footnote-195) It would seem that the operation was not entirely successful. Artificial intelligence and big data, often produced by connected devices (Internet of Things), enable online intermediaries to control a vast amount of information on the users’ activities and predict future behaviours. Monitoring, in the form of tracking and profiling (e.g. for behavioural advertising purposes), is commonplace. This questions the assumption whereby it would not be feasible for intermediaries to actively monitor all their users in order to prevent[[196]](#footnote-196) or react to unlawful activities. It is no coincidence that the European Commission recently presented guidelines to ‘facilitate and intensify the implementation of good practices for preventing, detecting, removing and disabling access to illegal content.’[[197]](#footnote-197) Moroever, the European Court of Human Rights made clear that intermediaries are often in the position to know about their users’ activities regardless of a formal notice[[198]](#footnote-198). This study brings empirical evidence that online platforms try to avoid liability even when they do have knowledge of the illegal activities of their users. More importantly, they violate privacy and freedom of expression, those same rights that would justify their immunity from liability.

**4. Privacy in the online private ordering of the internet of bodies**

In the IoB, privacy plays a key role in justifying the intermediary liability of the platforms, as well as the platform’s responsibility in terms of aestheric discrimination. Therefore, it is crucial to understand how privacy is regulated in the IoB.

Even though data protection and privacy are the object of hard laws,[[199]](#footnote-199) the ‘legals’ play an increasing role in the regulation of the relevant rights. Due to the pace of the technological evolution, the law cannot keep up.[[200]](#footnote-200) A consequence of this delay is that private actors fill the gaps (and sometimes purport to circumvent existing laws) by means of their ‘legals’, thus creating a private ordering of online relations.[[201]](#footnote-201) Most of the legals are US contracts rarely adapted to the EU context; more importantly, they are hardly legible, obscure and often non-enforceable.[[202]](#footnote-202) This is particularly alarming, since ‘data privacy law has been subsumed by consumer contract law.’[[203]](#footnote-203) The said features explain the so-called rational ignorance of those who do not read the privacy policies; indeed, it may be ‘rational to refrain from reading privacy policies if the costs of reading exceed the expected benefits of ignorance.’[[204]](#footnote-204) The readability has also immediate legal consequences in terms of remedies, since under the Unfair Terms Directive,[[205]](#footnote-205) the assessment of the unfair nature of the terms shall relate to the definition of the main subject matter of the contract and to the adequacy of the price or remuneration only insofar as the contract is not drafted in plain intelligible language.

Nearly 70 per cent of the respondents to the MSM survey admit not to read the ‘legals,’[[206]](#footnote-206) because they are too long, full of jargon, boring, irrelevant, and complicated (two of them blamed their own laziness or lack of patience). These features affect the core of privacy online; indeed ‘ambiguous language (…) undermines the purpose and value of privacy notices for site users.’[[207]](#footnote-207) Those who read the legals do so to be sure about their rights and obligations vis-à-vis the platform and other users (especially with regards to possibility of blocking and/or reporting other users). However, the same respondents are sometimes aware that ‘they're never run the way they say they are. I just like to know how well they pretend to protect you and how protected my data is.’[[208]](#footnote-208)

Those who read the legals claim to understand them or, at least, to be aware of the existence of the relevant policies, but they justify this with their education (PhD in Law) or the specific background and area of work. This is in line with the studies that found that ‘courts and laypeople can understand the same privacy policy language quite differently.’[[209]](#footnote-209) However, this could also be seen as another instance of when users’ self-perceived knowledge of their rights is high, but their actual knowledge is limited.[[210]](#footnote-210) While maintaing that they understand the legals of the MSM apps they use, they accept that ‘[t]hey're often extremely inaccessible in the way they're created and can still be full of holes.’[[211]](#footnote-211) It seems clear that the online social contract has weak foundations. However, one of the users suggests to re-design the legals by getting read to the mere link to the Terms of Service and Privacy Policy and, instead, ‘to give the user a few brief points of what terms they are agreeing to, especially ones relating to privacy.’ This solution can be seen as expression of the broader ‘awareness by design’[[212]](#footnote-212) trend. Hopefully, the privacy-by-design requirement under the GDPR[[213]](#footnote-213) will be interpreted as encompassing also the drafting of the legals. Embedding privacy in the design in this sense would mean short, clear, consistent, and engaging legals. Gamified interactions[[214]](#footnote-214) may constitute an important strategy therefor.

This might concur to explain the so-called privacy paradox, whereby ‘despite apparent high levels of concern about privacy risks, consumers often give up their privacy, sometimes for relatively low-level rewards.’[[215]](#footnote-215) Users do care about their privacy and, nonetheless, give away their personal data also because they are not in the position to understand their rights and obligations.[[216]](#footnote-216) The online social contract should be founded on a clear pact as to the parties’ rights and obligations; the readability of the legals may play an important role. Therefore, this author measured readability level, readability score, and text quality.[[217]](#footnote-217) The readability formulas taken into account as to the readability levels are the Flesch-Kincaid Grade Level,[[218]](#footnote-218) the Gunning-Fog Score,[[219]](#footnote-219) the Coleman-Liau Index,[[220]](#footnote-220) the SMOG Index,[[221]](#footnote-221) and Automated Readability.[[222]](#footnote-222) As to the readability score, I have referred to the Flesch-Kincaid Reading Ease,[[223]](#footnote-223) the Spache Score,[[224]](#footnote-224) and the New Dale-Chall Score.[[225]](#footnote-225) Considering the Terms of Service in isolation would be incorrect, since these incorporate also the privacy policy[[226]](#footnote-226) and the usage guidelines[[227]](#footnote-227). The results are as follows.

Grindr’s, PlanetRomeo’s, and Hornet’s legals consist respectively of 14,189, 7,537, and 6,342 words. The first and the last are very similar, including entire sentences which are taken *verbatim* from the other app’s legals. PlanetRomeo’s legals are quite different (probably because they are a European company) and do not include separate usage guidelines.

**Table 1. Readability level**

|  |  |  |  |
| --- | --- | --- | --- |
| Readability formula | Grindr | PlanetRomeo | Hornet |
| Flesch-Kincaid Grade Level | 13 | 10 | 10.6 |
| Gunning-Fog Score | 14.1 | 11.7 | 11.6 |
| Coleman-Liau Index | 13.8 | 13.6 | 13.3 |
| SMOG Index | 15.1 | 12.4 | 13.3 |
| Automated readability | 13.3 | 9.1 | 9.9 |
| Average Grade Level | 13.9 | 11.4 | 11.7 |

The desirable score would be 8. One can see that the Grindr legals are less readable according to all the tests, requiring at least college education. Since 59% of the users of dating apps do not have the sufficient level of education,[[228]](#footnote-228) one can infer that the majority of the users of MSM apps cannot understand the terms of their contractual relation with the platform. PlanetRomeo has the most readable legals, although Hornet performs better with regards to the Gunning-Fog Score and the Coleman-Liau Index. Even though Hornet does not score the highest in terms of readability *per se*, they have the shortest legals, which seems particularly important given the information overload that users experience online.[[229]](#footnote-229)

**Table 2. Readability score.**

|  |  |  |  |
| --- | --- | --- | --- |
| Readability formula | Grindr | PlanetRomeo | Hornet |
| Flesch-Kincaid Reading Ease | 41.1 | 48.4 | 48.2 |
| Spache Score | 4.1 | 3.3 | 3.9 |
| New Dale-Chall Score | 6.8 | 6.1 | 6.2 |

Given that the desirable score would be between 60 and 70, the Flesch-Kincaid Reading Ease shows that the legals of these apps are all difficult to read (college level). However, PlanetRomeo is, albeit not by much, the best, being the closest to’fairly difficult to read’ (10th to 12th grade). The Spache score should be disregarded because it is designed for children to the 4th grade and because using other calculators the output is radically different.[[230]](#footnote-230) Similarly, the New Dale-Chall Schore deems difficult the words that are not familiar to a US fourth grader, which one can imagine is not the typical user of MSM apps.[[231]](#footnote-231)

Therefore, the ranking as shown in Table 2 is the same as the one in Table 1. It is confirmed that Grindr’s legals are the least readable and PlanetRomeo’s ones are the most readable.

**Table 3. Text quality.**

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Grindr | PlanetRomeo | Hornet |
| Sentences > 30 syllables | 327 | 175 | 123 |
| Sentences > 20 syllables | 413 | 275 | 171 |
| Words > 4 syllables | 391 | 641 | 129 |
| Words > 12 letters | 151 | 79 | 61 |
| Passive voice count | 114 | 77 | 58 |
| Adverb count | 394 | 227 | 206 |

One more time, Grindr is the worst performer across the board, while PlanetRomeo has the best text quality. The fact that it has more words with more than 4 syllables is probably due to the name of the app itself being longer than the rivals’ ones, as well as to the use of some words in Dutch.[[232]](#footnote-232) Hornet’s text quality is superior to the competitors, but this may be due primarily to the quantitative datum of the length of its legals.

The above results present only a partial picture. Indeed, only the three companies’ own legals were assessed. However, by accessing the relevant services, the user will be bound also to other legals (e.g. Google’s ones as to analytics and/or advertising). Therefore, supposedly, the user should read and understand also a number of third parties’ legals, which means that the overall readability would further decrease.

In the unlikely event of a user reading and understanding the legals, the effort would soon be useless. Indeed, the legals are updated quite often and without proper notice.[[233]](#footnote-233) Of the legals analysed, Grindr was the only one clarifying the date of the terms and the main updated, but they did not made available the previous versions (unlike Google, for instance).[[234]](#footnote-234)

The low readability of the legals and the structural inequality of bargaining power also explain the privacy paradox. A European report[[235]](#footnote-235) found that the number of users who read the ‘legals’ would more than dounble in case of simple language and short text. One may object, however, that even though the legals are hard to understand and potentially unfair, this has no practical consequences because they are not enforced or they are enforced fairly (for instance, by allowing the immoral behaviour they declare to prohibit).[[236]](#footnote-236) The findings of this study suggest otherwise. Amongst the respondents who have an opinion and / or knowledge on the issue, 60 per cent believe that the legals are enforced and they are enforced unfairly.[[237]](#footnote-237) The rest believes that they are enforced, but fairly (two half of them state that there is an element of arbitrariness to the private enforcement). In turn, no one believes that the legals are not enforced in the first place.[[238]](#footnote-238)

**4.1. Beyond the form: do MSM app providers respect their users privacy?**

While the form of the legals can in itself be in breach of the GDPR,[[239]](#footnote-239) it is important to assess if their content confirms that the analysed intermediaries do not respect their users’ privacy. It has been already noted that MSM app providers betray their users’ privacy expectations by providing app store providers a back-door. A recent complaint[[240]](#footnote-240) lodged by the Norwegian Consumer Council (*Forbrukerrådet*) against Grindr confirms that MSM app providers’ behaviour may not be privacy-friendly.

First, an analysis of the functioning of Grindr and a number of interviews evidenced that Grindr screens each profile picture ex ante and reviews the profile descriptions (Fig. 2).[[241]](#footnote-241) The focus group confirmed that the practice of not authorising profile pictures is commonplace, which suggests that Grindr and similar apps put in place a strict filter.

The screening activities have a direct impact on the liability regime, because they put the intermediary in the position to know of the illegal activities carried out by the users in their profile descriptions or with their profile pictures. Now, prima facie one may think that if the national implementation of the eCommerce Directive is based on the notice-and-takedown system, then MSM app providers would not be liable for illegal content even if they have actual knowledge of it without needing a notice. However, under *Kaschke v Gray[[242]](#footnote-242)* blog owners cannot avail themselves of the hosting immunity if they can infer the existence of the infringing content from the checking of the spelling and grammar of the user-generated content. Applying this case to our scenario, it seems clear that MSM app providers filtering their users’ content cannot invoke the safe harbours. Conversely, a defensive strategy for said providers might be that their operation is entirely automatic and, therefore, without humans in the loop, no knowledge is possible.[[243]](#footnote-243) While one of the spokespersons of the MSM apps affirmed that there was a team of human beings reviewing the content,[[244]](#footnote-244) there is evidence that at least some platforms do put in place automated screening systems[[245]](#footnote-245) (Fig. 3).[[246]](#footnote-246)

In light of the increased use of AI and automated systems, it is arguable that *Davison* is no longer good law in that respect, otherwise every intermediary could escape all liability by automating the way they monitor their users and/or screen the user-generated content.

Second, regrettably, instead of precisely listing the data that Grindr accesses, they provide mere ‘examples of the types of data that we collect.’[[247]](#footnote-247) The interviewed users were surprised to find out that this data encompasses all the (supposedly) private messages, including all photos, location, audio, and video. From a purpose limitation[[248]](#footnote-248) and data retention perspective, it is noteworthy that the messages are retained indefinetely[[249]](#footnote-249) not only for archival purposes, but also ‘as otherwise allowed by law.’ Processing of personal data for purposes other than those for which consent was originally sought is allowed only for archiving, scientific, historical or statistical purposes.[[250]](#footnote-250) However, archiving falls within the scope only if ‘in the public interest,’[[251]](#footnote-251) which does not seem to apply to Grindr’s archiving. Moreover, this exception requires the putting in place of appropriate safeguards to ensure data minimisation, whilst Grindr seems to collect data way beyond what is strictly necessary for its operation.

It is impossible to fully understand which data Grindr is processing. To this end, this author sent Grindr a data subject access request in January 2018, but as of May 2018, they have not allowed said access yet.[[252]](#footnote-252)

Third, the GDPR strengthens the conditions for valid consent,[[253]](#footnote-253) as it must be given freely, informed, unambiguous, specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn.[[254]](#footnote-254) The only GDPR-compliant consent ‘is a tool that gives data subjects control over whether or not personal data concerning them will be processed.’[[255]](#footnote-255) This does not seem the case with Grindr. Indeed, the consent is expressed simply ‘by accessing’[[256]](#footnote-256) the service. Whilst this is hardly freely given[[257]](#footnote-257) and opt-in consent, this mechanism is particularly problematic with regards to the data on sex, sexual orientation, and health that Grindr processes. Indeed, the main legal basis for the processing of such sensitive personal data is *explicit* consent, which is the opposite of the *per-facta-concludentia* consent that seems the industry practice. Since regular consent requires already an affirmative action, it is unclear what explicit consent means. The Article 29 Working Party suggests that data subjects may explicitly consent ‘by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature.’[[258]](#footnote-258) The fact that Grindr processes both sensitive and non-sensitive personal data has an impact on its obligations with regards to both types of data. Indeed, consent is presumed not to be freely given if the data controller does not allow separate consent to different personal data operations, ‘despite it being appropriate in the individual case.’[[259]](#footnote-259) The processing of both sensitive and non-sensitive data seems an obvious example of separate consent. This said, whereas conduct (as opposed to statements or declaration) cannot deliver explicit consent, it could nonetheless be a form of expressing (non-explicit) consent.[[260]](#footnote-260) While the check box is not in itself invalid (see Fig. 4),[[261]](#footnote-261) consent must be informed, therefore a long and illegible[[262]](#footnote-262) document would not deliver GDPR-compliant consent, particularly if it is not clear for which purposes each type of data is processed.[[263]](#footnote-263)

Another problem with Grindr’s check box is that ‘consent must always be obtained before the controller starts processing personal data for which consent is needed.’[[264]](#footnote-264) However, this screen (Fig. 4) follows the request of the email address and the date of birth, which can constitute personal data (Fig. 5).[[265]](#footnote-265)

Granularity is another critical point. The Article 29 Working Party clarifies that if ‘consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given.’[[266]](#footnote-266) Grindr asks the users’ to accept the privacy policy separately to the terms of service. However, it is questionable whether non-negotiable privacy policies can ensure that consent is freely given. This is particularly evident with the data Grindr collects without them being necessary for the provision of the service, for instance the sharing of HIV status data with third parties.[[267]](#footnote-267)

Moreover, Grindr limits or even denies the exercise of the right to withdraw not only ‘if the law permits or requires us to do so’[[268]](#footnote-268), which it does not in the EU, but also ‘if we are unable to adequately verify your identity.’[[269]](#footnote-269) Aside from the fact that the GDPR does not provide any exceptions or limitations to the right of withdrawal, it is noteworthy that ‘(i)t shall be as easy to withdraw as to give consent.’[[270]](#footnote-270) Since it is not required to prove one’s identity when giving consent, equally this requirement shall not apply to the withdrawal. Moreover, data controllers should provide the same interface for giving and withdrawing consent,[[271]](#footnote-271) but it is unclear which interface one should use to exercise this right.

In April 2018, a complaint filed by the Norwegian Consumer Council against Grindr exposed these issues, with particular regards to the sharing of the data on sexual preferences with advertisers[[272]](#footnote-272) and the HIV status data with two analytics service providers. There are three strong arguments. First, Grindr declares that its users’ personal data may be processed in countries with weak data protection laws and, therefore, ‘you might be left without a legal remedy in the event of a privacy breach.’[[273]](#footnote-273) This chapter joins the Consumer Council[[274]](#footnote-274) in considering unfortunate the contractual provision on transnational data transfers because neither Grindr nor its parent company Beijing Kunlun Tech Co., Ltd. signed up to the Privacy Shield.[[275]](#footnote-275) Additionally, it is crucial to keep in mind that one of the main innovations of the GDPR is its extraterritorial application when goods or services are offered to data subjects in the EU or when these subjects’ behaviour is monitored.[[276]](#footnote-276) It would seem that Grindr both offers services to data subjects in the EU and monitors them, therefore it cannot leave these subjects without legal recourse.

The second argument is that data Grindr shares data about sexual orientation and sexual preferences through unencrypted data flows.[[277]](#footnote-277) This is in line with its Privacy Policy, whereby the company takes reasonable efforts to protect personal data from unauthorised access, yet ‘Grindr cannot guarantee the security of your Personal Data.’[[278]](#footnote-278) While the GDPR is technologically neutral, and, therefore, it does not mandate encryption, ‘the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.’[[279]](#footnote-279) In selecting the adequate security measures, companies must take into account the ‘state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.’[[280]](#footnote-280) When processing sensitive data, arguably, encryption should be the default security measure.

A third strong argument put forward by the Norwegiam Consumer Council is that ‘information about sensitive personal data being shared with third parties should not be hidden away in long terms of service and privacy policies.’[[281]](#footnote-281) This is in line with the Article 29 Working Party’s guidelines on consent according to which ‘information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions.’[[282]](#footnote-282) While users were surprised to find out that the data about their HIV status and sexual preferences were shared with third parties, this practice is not in itself unlawful. Therefore, the main issue is assessing if the consent asked by Grindr is of the quality required by the GDPR. As said above, arguably this is not the case, with the consent neither informed, freely given, granular, specific, let alone explicit.

The outrage[[283]](#footnote-283) that followed the news that Grindr shares HIV status and sexual preferences data with third parties is both a testament to the fact that the legals are not read or understood, as well as the fact that bottom-up pressures can be a very effective tool to improve data protection practices. Indeed, after claiming that this kind of sharing was industry practice, Grindr stated that they will refrain from the practice in the future.[[284]](#footnote-284) Interestingly, another justification put forward by the company was that if a user decides to disclose in their profile description, then this data is public.[[285]](#footnote-285) One should keep in mind that sensitive personal data is lawfully processed if manifestly made available to the public.[[286]](#footnote-286) However, the said outrage and the MSM survey confirmed that Grindr users see the platform as a private space.[[287]](#footnote-287) Grindr’s argument risks making people hide their HIV status, thus reinforcing HIV stigma.

Grindr’s response, moreover, is only partly convincing. First, the company will keep sharing data on sexual preferences with third parties including advertisers. Second, they have reassured that no third parties access profile data on Grindr; only ‘appropriate Grindr employees and trusted contractors’[[288]](#footnote-288) do and they are ‘bound by appropriate privacy and confidentiality terms.’[[289]](#footnote-289) This is at odds with the section of the Privacy Policy providing that both advertisers and partners use their own cookies or other tracking technology to collect personal data within the Grindr Services, while Grindr does ‘not control use of these tracking technologies.’[[290]](#footnote-290) It is not clear which data these third parties have access to, if not the profile data. One might conjecture that they have access to the ‘private’ messages, including the photographic content shared by the users.[[291]](#footnote-291)

The first challenge of the web, according to its inventor Sir Tim Berners-Lee, is the loss of control over personal data, which he relates also to the fact that ‘T&Cs are all or nothing.’[[292]](#footnote-292) This study showed that the quality of the legals of the MSM apps is an important element of this loss of control over one’s own personal data. The low quality of the ‘legals’ has practical consequences; one need only mention that consumers report problems with purchases related to the fact that they did not read and/or understand the terms of service.[[293]](#footnote-293) Ultimately, a fairer approach to data privacy and security would positively affect the consumers’ trust in the IoB (with increased profitability for the IoB providers).[[294]](#footnote-294) In the IoB environment, there are mostly data-fuelled, asymmetric, mass transactions; therefore, the main way to have a fairer private ordering of privacy is to make IoB providers understand that being privacy-friendly is a competitive advantage.[[295]](#footnote-295) If, in application of a joint interpretation of Data Protection by Design,[[296]](#footnote-296) accountability,[[297]](#footnote-297) and transparency,[[298]](#footnote-298) these providers changed the way they present the information about their users’ privacy (e.g. with visualisation tools and gamified interactions), they would contribute to laying the foundations for a more balanced online social contract. Thus, IoB providers would take up the recent Commission’s suggestion to provide a ‘clear, easily understandable and sufficiently detailed explanation of their content policy in their terms of service’,[[299]](#footnote-299) consistent the enhanced transparency principle as restated in the GDPR.[[300]](#footnote-300)

**5. Conclusions.**

In an IoB world, the body is becoming a key source of personal data. The body is changing the Internet like the Internet is changing the body, for instance in terms of cyborgisation and aesthetic discrimination. The body is no longer the sanctuary of the right to be left alone, which used to be the core of the right to privacy. In the IoB, as shown by this research, privacy has a fundamentally rhetorical function. On the one hand, it justifies the platforms’ immunity from liability, whilst on the other these same platforms force users to give away their privacy in the context of opaque and often unfair online transactions.

This research confirmed that in the online MSM community the body is heavily influenced by other users’ attitudes as well as by the MSM apps themselves. The profile descriptions openly excluding entire segments of population based on their appearance (e.g. no fats, no ‘femmes’) alongside the use of only certain pictures to advertise the services provided by MSM apps are just some examples of this.

MSM feel pressured to adapt to a certain model of body i.e. fit, young, masculine, and white. In excluding certain bodies, MSM users and apps reproduce heteronormative and capitalist values and power dynamics. The acceptable MSM is a highly productive and respectable member of the community who embraces and even exacerbates the male / female binary. The Internet would seem to offer an opportunity to dissociate physical body and gender identity, to the point that it was declared that ‘in cyberspace the transgendered body is the natural body’[[301]](#footnote-301) and that thanks to pseudonymity users may play with gender identity.[[302]](#footnote-302) This research presents evidence that the Internet does not overcome the gender binary and that in cyberspace the masculine, fit, white, abled body is the natural body. This is along the lines of the recent findings according to which the behaviour of young users online show a strong attachment to gender binarity.[[303]](#footnote-303)

Research showed that the ‘prevalence of weight/height discrimination is (…) comparable to rates of racial discrimination’[[304]](#footnote-304) and linked to this is the lack of laws preventing aesthetic discrimination. This chapter does not claim that racial discrimination is ontologically the same as aesthetic discrimination, but sometimes they are expressions of similar issues and prejudices and, in rethinking discrimination laws, new protected characteristics should be taken into account. Moreover, as intersectionality theory[[305]](#footnote-305) shows, different forms of discrimination and exclusion are in some way connected and overlap.[[306]](#footnote-306) Therefore, they cannot be understood and analysed in silos. Furthermore, the scenarios when discrimination is illegal should be broadened: there is no reason why discriminating against a disabled person as a member or guest of a private club or association is illegal, but doing so in an online community where the person spends a considerable amount of their time is not.[[307]](#footnote-307)

The analysis of the legals of MSM apps confirmed that users do not read them because they are too long and complicated. Obscure legals can hardly constitute the basis for the social contract of the IoB. It is proposed, however, that the data protection by design approach be interpreted jointly with transparency and accountability so as to encompass the design of the legals. These should be better drafted (short, clear, consistent) and they should stimulate the user’s attentiveness[[308]](#footnote-308) (e.g. through gamification, visualisation, etc.). Only if the IoB providers understand that privacy is a competitive advantage, the private ordering of privacy will become fairer.

Hidden in the contractual quagmire of the legals, there are provisions which are arguably unenforceable. MSM apps attempt to disclaim all liability for damages resulting from the interaction with the app or between the users, even when the app has knowledge of the illegal activity and even if this results in personal injury or death.[[309]](#footnote-309) While the exclusion or restriction of liability for death or personal injury resulting from negligence is obviously unenforceable under consumer protection legislation,[[310]](#footnote-310) the possibility to exclude liability when the intermediary has knowledge of the illegal activities carried out in the context of the intermediation would go against the letter and the spirit of the eCommerce Directive.

This study, finally, showed the ambiguous role played by privacy (or by its rhetorical use). The traditional justification for the immunity from intermediary liability (and the related lack of general monitoring obligation) is rooted in privacy and freedom of expression. This study brought evidence of an inconsistent reference to privacy. On the one hand, MSM apps claim to want to respect their users’ privacy and that, therefore, they do not monitor or have control over them. Thus, they create the preconditions for invoking immunity from intermediary liability on grounds of lack of knowledge. On the other hand, they act as an online police, allowing only certain user-generated content and only certain behaviours (e.g. by excluding everything which is deemed immoral). They blame it on the app store providers, which would not make their apps available if they would not comply with Apple’s and Google’s guidelines. However, secretly allowing the app stores providers to monitor the MSM apps’ users is in violation of these users’ privacy. MSM will have to opt: either actually respecting their users’ privacy and freedom of expression, thus placing themselves in the position to invoke immunity from intermediary liability, or keep controlling and monitoring their users, in which case they will not be able to exclude liability in the event of knowledge of illegal behaviours. Arguably, if privacy were a mere smokescreen, the justification for not making the intermediary liability stricter would no longer be tenable.

To conclude, the IoB promises more efficient and interconnected bodies. However, there are a number of privacy and ethical issues that cannot be overlooked. In the IoB, we are losing control over the body for at least three reasons. First, the perception of our body is heavily influenced by our online experience, for instance while using dating apps. Second, businesses are realising that the body is the most important source of personal data and they are endeavouring to extract them in ways which are often unfair and opaque. Third, smart devices do not only measure our biometric parameters, but also directly affect them (e.g. with implantable technologies), Now, in the *Capital*, Marx describes the labourer as nothing else than labour-power ‘devoted to the self-expansion of capital.’[[311]](#footnote-311) The fact that the time ‘for free-play of his bodily and mental activity’[[312]](#footnote-312) is taken away from the labourer is a major enslaving factor. The Internet of Things[[313]](#footnote-313) and the circular economy[[314]](#footnote-314) are leading to the death of the ownership related to the loss of control over our goods,[[315]](#footnote-315) with the IoB we risk being stripped of the last thing we used to own: our body. This may be the dawn of a new proletariat.

1. \* Guido Noto La Diega, PhD is Senior Lecturer in Cyber Law and Intellectual Property at the Northumbria University, where he is European Research Partnerships Coordinator (Law) and Co-convenor of NINSO The Northumbria Internet & Society Research Group. He is also Fellow of the Nexa Center for Internet & Society and Director of Ital-IoT Centre of Multidisciplinary Research on the Internet of Things. The author thanks the anonymous reviewers for the most helpful comments.The Ethics Committee of the Northumbria University, Faculty of Business and Law, approved this research. [↑](#footnote-ref-1)
2. Even though the relevant providers increasingly market these apps as social networks and even though this approach is followed by some scholars (e.g. Brandon Miller, ‘"They’re the modern-day gay bar": Exploring the uses and gratifications of social networks for men who have sex with men’ (2015) 51 Computers in Human Behavior 476), the way most of the analysed apps are designed suggest to prefer the generic ‘app’ and ‘platform’ terms, because they often lack of dedicated communal spaces where users can actually socialise and interact. Of the analysed apps, only Hornet has proper social features. Chad van de Wiele and Stephanie Tom Tong, ‘Breaking boundaries: the uses & gratifications of Grindr’ (2014) UbiComp ’14 Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquituous Computing 619 refer to ‘people-nearby applications’. Though it correctly emphasises the geographical element of these apps, it does not give account of those apps (such as PlanetRomeo) that enable to set a fictional location. Moreover, with minor exceptions (Joey Chiao-Yin Hsiao and Tawanna R Dillahunt, ‘**People-Nearby Applications: How Newcomers Move Their Relationships Offline and Develop Social and Cultural Capital’ (2017) CSCW ’17 Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing 26**), it does not seem that this phrase has been adopted in the relevant literature. [↑](#footnote-ref-2)
3. This is not to say that sex or dating are the only reasons why users engage with this kind of apps. Indeed, users resort to these apps (which one can call ‘dating apps’ for ease of reference) for a number of reasons, including seeking friendship, entertainment, and preparing for travelling. Elisabeth Timmermans and Elien De Caluwé, ‘Development and validation of the tinder motives scale (TMS)’ (2017) 70Computers in Human Behavior 341 present 13 motives for using Tinder. See also M Hobbs, S Owen, and L Gerber, ‘Liquid love? Dating apps, sex, relationships and the digital transformation of intimacy’ (2017) 53(2) Journal of Sociology 271; SR Sumter, L Vandenbosch and L Ligtenberg, ‘Love me Tinder: Untangling emerging adults’ motivations for using the dating application Tinder’ (2017) 34(1) Telematics and Informatics 67; CJ Carpenter and B McEwan, ‘The players of micro-dating: Individual and gender differences in goal orientations toward micro-dating apps’ (2016) 21(5) First Monday. [↑](#footnote-ref-3)
4. ‘Men who have sex with men’ (MSM) is a definition used traditionally in the medical research on HIV (see Michael W. Ross, ‘Men who have sex with men’ (1992) 4(4) AIDS Care 457). Here it is preferred to LGBT (or similar acronyms) because it does not make the assumption that those who use MSM apps identify themselves as gay or bisexual. It is increasingly accepted that two men can have sexual intercourse without necessarily being considered (or considering themselves) as homo- or bisexual (see, for instance, Jane Ward, *Not Gay: Sex Between Straight White Men* (New York: NYU Press, 2015), who shows that sex between men has always been a regular feature of heterosexual life). Queer is equally problematic, for instance because originally it was a derogatory term and many people still feel offended by it (one of the respondents to the survey used for this chapter openly complained about the use of the term ‘queer’, which was initially used as the title of the survey). There is not an umbrella term which encompasses all the nuances of sexuality and gender. MSM, for instance, may be seen as exclusive of agender and asexual people. However, apps like Grindr, Hornet and Romeo are hypersexualised and gender-polarised. Therefore, MSM seems the label that better encompasses the vast majority of the users of the analysed apps. [↑](#footnote-ref-4)
5. ***Scarlet Extended SA v SABAM*** [2011] ECR I-11959. [↑](#footnote-ref-5)
6. See, for instance, Daphne Keller, ‘The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation’ (*SSRN*, 8 February 2017) 64 <ssrn.com/abstract=2914684> accessed 25 September 2017, according to whom ‘the eCommerce rule against making [online service providers] monitor users’ communications protects both information and privacy rights of Internet users.’ [↑](#footnote-ref-6)
7. This seems to be the latest development of the Internet of Things. The IoB was the theme of the Computers, Privacy Data Protection conference of January 2018 (CPDP 2017). The idea of an ‘Internet of Bodies’ had been suggested, for instance, by Meghan Neal, ‘The Internet of Bodies Is Coming, and You Could Get Hacked’ (Motherboard Vice, 13 March 2014) <motherboard.vice.com/en\_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked> accessed 25 September 2017, who predicted that in 25 years traditional smart devices will be obsolete because ‘[c]omputers will become so tiny they can be embedded under the skin, implanted inside the body, or integrated into a contact lens and stuck on top of your eyeball.’ An example of the increasing demand for an expertise in this field is provided by the research carried out by Ghislaine Boddington, University of Greenwich (see, for instance, her pioneering workshop on ‘Virtual Physical Bodies’ (17-19 September 1999), ResCen, Middlesex University, London). [↑](#footnote-ref-7)
8. This dichotomy shapes also the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016] OJ L119/1. See, for instance, Article 13 on the information to be provided where personal data are collected from the data subject and Article 14 on the information to be provided where personal data have not been obtained from the data subject. Building on the GDPR’s approach, Gianclaudio Malgieri, ‘Property and (Intellectual) Ownership of Consumers’ Information: A New Taxonomy for Personal Data’ (2016) 4 PinG 133 suggests to distinguish between strong relationship data (data provided directly by customers), intermediate relationship data (data observed or inferred and related to the present life of consumers), and weak relationship data (predictive data). [↑](#footnote-ref-8)
9. For some critical remarks, see Jesse Emspak, ‘Should Apple iPhone X Trust Facial Recognition for Security?’ (*Scientific American*, 22 September 2017) <www.scientificamerican.com/article/should-apple-iphone-x-trust-facial-recognition-for-security/> accessed 25 September 2017. [↑](#footnote-ref-9)
10. Even though smart devices are increasingly implanted in our bodies, Katina Michael, ‘Mental Health, Implantables, and Side Effects’ (2015) 34(2) IEEE Technology and Society Magazine, 5, 6, denounces the ‘lack of qualitative research being conducted across the spectrum of implantable devices in the health sector.’ On biometrics and physical privacy, see Nancy Yue Liu, *Bio-Privacy: Privacy R*eg*ulations and the Challenge of Biometrics* (Abingdon: Routledge, 2012) 79-81. [↑](#footnote-ref-10)
11. cf Deborah Lupton, ‘Donna Haraway: The Digital Cyborg Assemblage and the New Digital Health Technologies’ in Fran Collyer (ed), *The Palgrave Handbook of Social Theory for the Sociology of Health and Medicine* (Basingstoke: Palgrave Macmillan 2015) 567. [↑](#footnote-ref-11)
12. See, for instance, Jeffrey H. Reiman, ‘Privacy, Intimacy, and Personhood’ (1976) 6(1) Philosophy & Public Affairs 26, 43, where he says ‘I come to view myself as the kind of entity that is entitled to the social ritual of privacy. That is, I come to believe that this body is mine in the moral sense.’ [↑](#footnote-ref-12)
13. Moira Gatens, ‘Privacy and the Body: The publicity of affect’ in Beate Rössler (ed), *Privacies: Philosophical Evaluations* (Palo Alto: Stanford University Press, 2004) 113 (the amorphous referring to privacy and the inchoate to the body). Gatens analysis, albeit interesting, is here overlooked because of its philosophical and literary take. [↑](#footnote-ref-13)
14. Xiaolin Wu and Xi Zhang, ‘Automated Inference on Criminality using Face Images’ (*arXiv*, 13 November 2016) <arxiv.org/pdf/1611.04135v1.pdf> accessed 25 September 2017. [↑](#footnote-ref-14)
15. *ibid* 2. [↑](#footnote-ref-15)
16. The main reference is to Cesare Lombroso, *L’uomo delinquente* (Milan: Hoepli, 1876). For a scholarly translation, see Cesare Lombroso, *Criminal man* (Durham: Duke University Press, Eng tr, 2006). [↑](#footnote-ref-16)
17. Suzanne Bell, ‘Lombroso, Cesare (1835-1909), in: *A Dictionary of Forensic Science* (Oxford: OUP, 2012). The system was refined by Alphonse Bertillon, who developed the first systematic biometric method to supposedly identify criminals. [↑](#footnote-ref-17)
18. cf Mary Gibson, ‘Forensic psychiatry and the birth of the criminal insane asylum in modern Italy’ (2014) 37(1) International Journal of Law and Psychiatry 117, 118. [↑](#footnote-ref-18)
19. Philip K. Dick, *The Minority Report* (1956;Gollancz: London, 2002). [↑](#footnote-ref-19)
20. Yilun Wang and Michal Kosinski, ‘Deep neural networks are more accurate than humans at detecting sexual orientation from facial images’ (Open Science Framework, 7 September 2017) <osf.io/zn79k/> accessed 25 September 2017. On some shortcomings and biases of this research see Antonio Casilli, ‘Une intelligence artificielle révèle les préjugés anti-LGBT (et anti-plein d'autres gens) des chercheurs de Stanford’ (*Casilli*, 9 September 2017) <www.casilli.fr/2017/09/09/une-intelligence-artificielle-revele-les-prejuges-des-chercheurs-de-stanford-envers-gays-biais-racisme/> accessed 25 September 2017. [↑](#footnote-ref-20)
21. Wang (n 19) 6. [↑](#footnote-ref-21)
22. Henry Havelock Ellis and John Addington Symonds, *Sexual Inversion* (1897, Basingstoke: Palgrave Macmillan, 2008). [↑](#footnote-ref-22)
23. Siobhan Somerville, ‘Scientific Racism and the Emergence of the Homosexual Body’ (1994) 5(2) Journal of the History of Sexuality 243, 248-249. [↑](#footnote-ref-23)
24. Homosexuality is punished with the death penalty in Afghanistan, Brunei, Mauritania, Sudan, Northern Nigeria, Yemen, Saudi Arabia, Somalia, Iran, Pakistan, Islamic State of Iraq and the Levant, Somaliland, Palestine (Gaza), United Arab Emirates, and Qatar. However, there is no evidence of enforcement in the last two countries; see, Aengus Carroll (ed), *State-sponsored homophobia* (Geneva: ILGA, 11th ed, 2016) 37. [↑](#footnote-ref-24)
25. Jean-Luc Jucker and others, ‘The effect of the thin body ideal in a media-naïve population’ (*bioXriv*, 14 August 2017) <www.biorxiv.org/content/biorxiv/early/2017/08/14/176107.full.pdf> accessed 25 September 2017. [↑](#footnote-ref-25)
26. Van de Wiele (n 1) 619. [↑](#footnote-ref-26)
27. Jody Farnden, Ben Martini, and Kim-Kwang Raymond Choo, ‘Privacy risks in mobile dating apps’ (2015) <arxiv.org/abs/1505.02906> accessed 3 June 2018. [↑](#footnote-ref-27)
28. See, e.g. *Herrick v Grindr, LLC*, No. 1:2017cv00932 - Document 63 (S.D.N.Y. 2018); *Saponaro v Grindr, LLC*, 93 F. Supp. 3d 319, 323 (D.N.J. 2015). [↑](#footnote-ref-28)
29. This seems to be true both for human beings and some animals; cf Michelle E.H. Helinski and Laura C. Harrington, ‘Male Mating History and Body Size Influence Female Fecundity and Longevity of the Dengue Vector *Aedes a*eg*ypti*’ (2011) 48(2) J Med Entomol 202. [↑](#footnote-ref-29)
30. Suffice to say, that studies that compared homosexual and heterosexual men found that in homosexual men the discrepancy between their current body and the body they believed they should have to attract a dating partner is significantly greater than the discrepancy between their current and ideal body types. See Lauren M. Fussner and April R. Smith, ‘It’s Not Me, It’s You: Perceptions of Partner Body Image Preferences Associated with Eating Disorder Symptoms in Gay and Heterosexual Men’ (2015) 62(10) Journal of Homosexuality 1329. On a pop note, it is no coincidence that Grindr’s first web series – ‘What the Flip’ – is focusing on body shaming and discrimination against Asian guys. See INTO Editors, ‘Dating as a Different Body Type’ (*Into*, 14 September 2017) <intomore.com/videos/dating-as-a-different-body-type/57402b4c71dc4258> accessed 27 September 2017. [↑](#footnote-ref-30)
31. Alan Downs, *The Velvet Rage: Overcoming the Pain of Growing Up Gay in a Straight Man’s World* (Cambridge: Da Capo Press, 2012) 190. [↑](#footnote-ref-31)
32. *ibid* 190. [↑](#footnote-ref-32)
33. Glen S Jankowski et al., ‘“Appearance potent”? A content analysis of UK gay and straight men’s magazines’ (2014) 11(4) Body Image 474. [↑](#footnote-ref-33)
34. # Participant to a recent survey indicated that it was ‘desirable’ or ‘essential’ that their potential partner was good-looking (92% vs. 84%) and had a slender body (80% vs. 58%). Melissa R. Fales et al., ‘Mating markets and bargaining hands: Mate preferences for attractiveness and resources in two national U.S. studies’ (2016) 88 Personality and individual differences 78.

    [↑](#footnote-ref-34)
35. Michael J. Rosenfeld and Reuben J. Thomas, ‘Searching for a Mate: The Rise of the Internet as a Social Intermediary’ (2012) 77(4) American Sociological Review 523. They also found that partnership rate has increased during the Internet era for same-sex couples, but ‘(u)nlike the partnership rate of gays and lesbians, overall adult partnership appears not to have changed during the Internet era’ (*ibid* 542). [↑](#footnote-ref-35)
36. *ibid*. 532. The cited study would probably need an update; it would not be surprising if the situation had changed due to the use of apps like Tinder and OKCupid becoming commonplace. Future research shall address these questions. [↑](#footnote-ref-36)
37. The relationship between privacy and MSM can be analysed also from other angles. For instance, it has been noted that the European Court of Human Rights has advanced the protection of LGBT people mainly relying on the right to privacy (eg European Convention of Human Rights, art 8. See, for instance, *Oliari* v *Italy* Apps nos 18766/11 and 36030/11 (ECHR, 31 July 2015) and this is the very reason why the Court never recognised the right to marriage, which is a right on the public stage. See Frances Hamilton, ‘The Case for Same-Sex Marriage Before the European Court of Human Rights’ (Journal of Homosexuality, 26 September 2017) <www.tandfonline.com/doi/full/10.1080/00918369.2017.1380991> accessed 27 September 2017. [↑](#footnote-ref-37)
38. ‘Online dating’ (*Statista*, 2018) <www.statista.com/outlook/372/100/online-dating/worldwide#> accessed 2 June 2018. [↑](#footnote-ref-38)
39. Revenues for US$590m have been generated in the US in 2018 (ibid) . [↑](#footnote-ref-39)
40. 7Park Data ‘Love in the Time of Apps: Dating app user behaviour report’ (*7Park Data*, February 2017) <info.7parkdata.com/dating-report-2017?portalId=447976&hsFormKey=e8588e233d311b2c5434d5899dfe5b99&submissionGuid=d751da3e-09d9-4aeb-9503-db6b1f8271ae#wizard\_module\_245004896088576082163332572113761706729> accessed 25 September 2017. [↑](#footnote-ref-40)
41. The Norwegian Consumer Council filed a complaint against Grindr because of this. *Forbrukerrådet*, complaint of 3 April 2018. The text is available in English at [<fil.forbrukerradet.no/wp-content/uploads/2018/04/2018-04-03-complaint-grindr.pdf](https://fil.forbrukerradet.no/wp-content/uploads/2018/04/2018-04-03-complaint-grindr.pdf)> accessed 3 May 2018. [↑](#footnote-ref-41)
42. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. [↑](#footnote-ref-42)
43. **‘**Most popular dating apps in the United States as of April 2016, by market share’ (*Statista*, 2016) <www.statista.com/statistics/737081/popular-online-dating-market-share-users-monthly/> accessed 2 June 2018. [↑](#footnote-ref-43)
44. For the focus on location data and purpose limitation, see the interesting work of Michael Herrmann and others, ‘Privacy in Location-Based Services: An Interdisciplinary Approach’ (2016) 13(2) SCRIPTed 144. On trilateration to figure out the location of the targeted victim even when the "hide distance" function is enabled see Nguyen Phong Hoang, Yasuhito Asano, and Masatoshi Yoshikawa, ‘Your neighbors are my spies: Location and other privacy concerns in dating apps’ (2016) 18th International Conference on Advanced Communication Technology 715. See also Hao Dang, Stephanie Cai, and Xuanning Lang, ‘Location-based gay communication: An empirical study of smartphone gay apps use in Macau’ (*SSRN*, 27 April 2013) <ssrn.com/abstract=2257253> accessed 27 September 2017 about location-based services for MSM, but they overlook the privacy-related issues. [↑](#footnote-ref-44)
45. See Arno R. Lodder, ‘When ‘there’ can be everywhere: On the cross-border use of WhatsApp, Pandora, and Grindr’ (2014) 5(2) European Journal of Law and Technology 1. A partial exception is Kristian Møller Jørgensen, ‘The mediatization of public sex cultures in the case of the hook-up app Grindr’ (ECREA 2016 conference, Prague, November 2016), in that he states that ‘(a)long with the normalisation of geo-locative dating and hook-up practices in mainstream publics (…) imaginations of sexual privacy and indeed publicness seem to be changing.’ However, in that paper privacy is understood as a sociological concept and the real focus is on publicness. Similarly, Evangelos Tziallas, ‘Gamified Eroticism: Gay Male ‘Social Networking’ Applications and Self-Pornography’ (2015) 19 Sexuality & Culture 759, 769, conceptualises the interactions on MSM apps as porn and asserts that this fundamentally altered inter alia the meaning of privacy. [↑](#footnote-ref-45)
46. Conversely, health-related research is already quite developed. In particular, some scholars underline that Grindr and similar apps increase the risk of HIV/STIs transmission. See, for instance, ER Burrell et al, ‘Use of the location-based social networking application GRINDR as a recruitment tool in rectal microbicide development research’ (2012) 16 AIDS and Behavior 1816; Raphael Landovitz et al., ‘Epidemiology, Sexual Risk Behavior, and HIV Prevention Practices of Men who Have Sex with Men Using GRINDR in Los Angeles, California’ (2013) 90(4) Journal of Urban Health 729; Hailey Winetrobe et al., ‘Associations of unprotected anal intercourse with Grindr-met partners among Grindr-using young men who have sex with men in Los Angeles’ (2014) AIDS Care 1. More recently, Lixuan Zhang, Iryna Pentina and Wendy Fox Kirk, ‘Who uses mobile apps to meet strangers: The roles of core traits and surface characteristics’ (2017) Journal of Informational Privacy and Security, have underlined that there are mainly two streams of research around dating apps. On the one hand, studies of the motivations for using this kind of apps (e.g. Hobbs (n 2)). On the other hand, research on who uses dating apps (e.g. Barış Sevi, Tuğçe Aral and Terry Eskenazi, ‘Exploring the hook-up app: Low sexual disgust and high sociosexuality predict motivation to use Tinder for casual sex’ (2017) Personality and Individual Differences). [↑](#footnote-ref-46)
47. Christoph Lutz and Giulia Ranzini, ‘Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder’ (2017) 3(1) Social Media + Society 1. [↑](#footnote-ref-47)
48. cf Chris Ashford, ‘Queer theory, cyber-ethnographies and researching online sex environments’ (2009) 18(3) C.T.L. 297; Dang (n 33); Lodder (n 34); Kyle Jamie Fisher, ‘Grindr: An investigation into how the remediation of gay ‘hook up’ culture is converging homosexual digital spaces and heterosexual physical spaces’ (*Academia.edu*, 2015) <www.academia.edu/29176885/Grindr\_An\_investigation\_into\_how\_the\_remediation\_of\_gay\_hook\_up\_culture\_is\_converging\_homosexual\_digital\_spaces\_and\_heterosexual\_physical\_spaces> accessed 27 September 2017; Joseph Lawless, ‘The politicizing of the femme fatale: Negotiations of gender performativity in the digital space’ (Columbia Law School, Autumn 2015) <www.academia.edu/28712568/The\_Politicizing\_of\_the\_Femme\_Fatale\_Negotiations\_of\_Gender\_Performativity\_in\_the\_Digital\_Space> accessed 27 September 2017; Kristian Møller Jørgensen, ‘Boundary works of Grindr research: Sociological and queer perspectives on shame and intimacy’ (AoIR 2016 conference, Berlin, October 2016). [↑](#footnote-ref-48)
49. On privacy and MSM apps, however, see Hoang (n 33). [↑](#footnote-ref-49)
50. Since MSMs do not necessarily identify as non-heterosexual, it would be inaccurate to describe apps such as Tinder and POF as ‘heterosexual’ dating apps. [↑](#footnote-ref-50)
51. However, privacy and non-MSM dating apps there is a growing body of literature. See, for instance, Rory D Bahadur, ‘Individual Sovereignty, Freer Sex and Diminished Privacy: How an Informed and Realistic Modern Sexual Morality Provides Salvation from Unjustified Shame’ (2016) 8(2) Elon Law Review 245, on the increasingly publicised heterosexual female sexuality, mainly related to dating apps and, more generally, the Internet. See also Farnden (n 26); Lutz (n 36); Kath Albury, Jean Burgess, Ben Light, Kane Race, and Rowan Wilken, ‘Data cultures of mobile dating and hook-up apps: Emerging issues for critical social science research’ (2017) 4(2) Big Data & Society 1. [↑](#footnote-ref-51)
52. Once performed the test, it appeared clear that the Spache Score and the New Dale-Chall Score are not suitable for the analysis of the legals because are designed having in mind children of the elementary school. [↑](#footnote-ref-52)
53. From 20 March 2017 to 20 September 2017. [↑](#footnote-ref-53)
54. The participation to the survey has not been actively solicited. The potential participants contacted this author, whose profile clearly stated the research-related purpose of the account. After some introductory explanations on the survey, the relevant link was sent only after the potential respondent expressed their agreement. The survey could not be completed if not after reading and accepting the participant information and debrief sheet. [↑](#footnote-ref-54)
55. The main focus is on Grindr, which is the most important MSM app, described as ‘the

    hook-up app that my sexual biography as a gay man is inseparable of’ (Jørgensen (n 34) 1). [↑](#footnote-ref-55)
56. A poll with over 2000 respondents found that Grindr, Scruff, Hornet, Tinder, Jack’d, and PlanetRomeo are the most used MSM apps (Travel Gay Asia and Gay Star News, ‘Gay dating apps survey 2016’ (*Travel Gay Asia*, 1 December 2016) <https://www.travelgayasia.com/gay-dating-apps-survey-2016/> accessed 28 September 2017. This author had created an ad-hoc profile to study also Jack’d, but this company suspended his account, possibly because it was deemed to be an attempt of unauthorised advertising. Tinder was left out because it is not limited to MSM dating. [↑](#footnote-ref-56)
57. See e.g. BL Berg and H Lune, Qualitative research methods for the social sciences (8th edn Pearson Boston 2011. [↑](#footnote-ref-57)
58. MB Miles and AM Huberman AM, *Qualitative data analysis: An expanded sourcebook* (2nd ed, Sage 1994) 26 [↑](#footnote-ref-58)
59. (MQ Patton, *Qualitative research and evaluation methods* (3rd ed, Sage 2002) 36 as cited by , Lawrence A Palinkas, Sarah M Horwitz, Carla A Green, Jennifer P Wisdom, Naihua Duan, and Kimberly Hoagwood, ‘Purposeful sampling for qualitative data collection and analysis in mixed method implementation research’ (2015) 42(5) Administration and Policy in Mental Health and Mental Health Services Research 533). [↑](#footnote-ref-59)
60. *Cf* Judee K. Burgoon, ‘Privacy and Communication’, in Michael Burgoon (ed), *Communication Yearbook 6* (Abingdon: Routledge, 1982) 206, 213; JL Cohen, ‘Rethinking Privacy: Autonomy, Identity, and the Abortion Controversy’ in Jeff Alan Weintraub and Krishan Kumar*, Public and private in thought and practice: perspectives on a grand dichotomy* (Chicago: University of Chicago Press, 1997) 161; Rosamund Scott, *Rights, Duties and the Body. Law and Ethics of the Maternal-Fetal Conflict* (London: Hart, 2002) 195. [↑](#footnote-ref-60)
61. Philip Brey, ‘The importance of workplace privacy’ in Sven Ove Hansson and Elin Palm (eds), *The Ethics of Workplace Privacy* (Bern: Pieter Lang, 2005) 97, 102 [↑](#footnote-ref-61)
62. As noted by Tom Penney, ‘Faceism and Fascism in Gay Online Dating’ (*32 Queer Networks*, 2017) <dpi.studioxx.org/en/no/32-queer-networks/faceism-and-fascism-gay-online-dating per centE2 per cent80 per centA8> accessed 27 September 2017, it ‘is startling how aggressively defensive and entitled profiles are; ‘masc only, no fems’, ‘don’t contact me if…’, ‘no asians,’ which altogether constructs an environment of hostility and exclusion before-the-fact.’ [↑](#footnote-ref-62)
63. Senthorun Raj, ‘Grindring for justice’ (Right Now, 21 March 2016) <rightnow.org.au/essay/grindring-for-justice/> accessed 27 September 2017. [↑](#footnote-ref-63)
64. # Nathalie Dens, Patrick De Pelsmacker, Wim Jannsens, ‘Effects of Scarcely Dressed Models in Advertising on Body Esteem for Belgian Men and Women’ (2009) 60(5-6) Sex Roles 366.

    [↑](#footnote-ref-64)
65. Carl Bonner-Thompson, ‘”The meat market”: production and regulation of masculinities on the Grindr grid in Newcastle upon-Tyne, UK’ (2017) Gender, Place & Culture 3. [↑](#footnote-ref-65)
66. ibid 3. [↑](#footnote-ref-66)
67. Jankowski (n 31) 474. [↑](#footnote-ref-67)
68. Bonner-Thompson (n 63) 1. [↑](#footnote-ref-68)
69. This is not to say that nudity in itself cannot be considered positive in terms of liberation from social constructions and taboos. [↑](#footnote-ref-69)
70. These are the screenshots of ten randomly selected torsos shown on Grindr on 28 September 2017 in Newcastle upon Tyne. The randomisation was done by launching the app and selecting the first 10 profile pictures of torsos. Most of them can be considered fit, young, white, and masculine. [↑](#footnote-ref-70)
71. # Body dissatisfaction associated to dating is not exclusive to MSM relationships. For instance, it was found that there is ‘a relationship between importance of popularity with boys and body dissatisfaction (which is) fully mediated by the belief that boys see thinness as important in rating girls' attractiveness.’ (Susan J. Paxton et al., ‘Body Dissatisfaction, Dating, and Importance of Thinness to Attractiveness in Adolescent Girls’ (2005) 53(9-10) Sex Roles 663; similarly, see Carolyn Tucker Halpern et al., ‘Effects of body fat on weight concerns, dating, and sexual activity: A longitudinal analysis of Black and White adolescent girls’ (1999) 35(3) Developmental Psychology 721). Research suggests that ‘homosexual men and women have similar mate preferences to heterosexual men and women by showing more dating desire for attractive and high social status persons’ (Thao Ha et al., ‘Effects of Attractiveness and Status in Dating Desire in Homosexual and Heterosexual Men and Women’ (2012) 41(3) Archives of Sexual Behavior 673). Future research should further address similarities and differences between MSM and heterosexual dating.

    [↑](#footnote-ref-71)
72. Michael D. Bartone, ‘Jack’d a Mobile Social Networking Application and Gender Performance: A Site of Exclusion within a Site of Inclusion’ (2018) 65(4) Journal of Homosexuality 501. The cited research, however, does not clearly allocate the responsibility for this phenomenon. [↑](#footnote-ref-72)
73. For a recent research that sheds new light on the issue, see Karen Lumsden and Heather Morgan, ‘Media framing of trolling and online abuse: silencing strategies, symbolic violence, and victim blaming’ (2017) Feminist Media Studies, that focus on online behaviours related to trolling including body shaming. For an application to the MSM realm, see Supercup, ‘The Ugly Truth of Body Shaming in the Gay Press’ (*HuffingtonPost*, 18 April 2017) <www.huffingtonpost.com/entry/the-ugly-truth-of-body-shaming-in-the-gay-press\_us\_58f63545e4b048372700dba1> accessed 25 September 2017. [↑](#footnote-ref-73)
74. Jason S. Wrench and Jennifer L. Knapp, ‘The Effects of Body Image Perceptions and Sociocommunicative Orientations on Self-Esteem, Depression, and Identification and Involvement in the Gay Community’ (2008) 55(3) Journal of Homosexuality 471 denounced the negative effects of this phenomenon and noted that males report ‘higher levels of image fixation, antifat attitudes, dislike of fat people, weight locus of control (indicating internal loci), physical discrimination, weight discrimination, and depression’ (*ibid* 496). [↑](#footnote-ref-74)
75. See the pioneering work of Raul C. Schiavi, *Aging and male sexuality* (Cambridge: CUP, 1999) and the more recent Imani Woody, ‘Aging Out: A Qualitative Exploration of Ageism and Heterosexism Among Aging African American Lesbians and Gay Men’ (2013) 61(1) Journal of Homosexuality 145. [↑](#footnote-ref-75)
76. Internalised homophobia can be described as the internalisation of the mythology and opprobrium which characterise current social attitudes towards homosexuality (Alan K. Malyon, ‘Psychotherapeutic Implications of Internalized Homophobia in gay men’ (1982) 7(2-3) Journal of Homosexuality 59, 60). For the relation of this concept to shame and self-esteem see David J. Allen and Terry Oleson, ‘Shame in Internalized Homophobia in Gay Men’ (1999) 37(3) Journal of Homosexuality 33. [↑](#footnote-ref-76)
77. ## Some authors claim that asexual people reinforce ableism by distancing themselves from people with disabilities (Karen Cuthbert, ‘You Have to be Normal to be Abnormal: An Empirically Grounded Exploration of the Intersection of Asexuality and Disability’ (2017) 51(2) Sociology 241).

    [↑](#footnote-ref-77)
78. The classical ‘no fats, no femmes, no Asians’ slogan, that one can find in many profile descriptions of users of MSM apps, does not seem a mere expression of taste (which may be something along lines of ‘I am looking for’ or ‘I am into’). Conversely, the focus of these profile descriptions is to exclude entire segments of the community in the essentialist belief that, say, all non-masculine users are the same. The writer-director Vince Ha turned that sadly popular phrase into the film *No Fats, No Femmes, No Asians*, presented in Toronto on 14 June 2017. Similarly, it has been noted that ‘(w)e tend to think our preferences are natural and fixed when, in fact, they may be more plastic and susceptible to structural influences than we imagine’ (Russell K. Robinson, ‘Structural dimensions of romantic preferences’ (2008) 76 Fordham Law Review 2787). [↑](#footnote-ref-78)
79. This author is not affirming, however, that one should oblige oneself to change whom one is attracted to. One can agree with Raj (n 61), where he says that ‘we will always find specific features about a person sexy. But, it is how we express those desires and the space we give others to shape their own pleasures that we must be more vigilant about and attentive towards.’ [↑](#footnote-ref-79)
80. Lawless (n 37) 1. [↑](#footnote-ref-80)
81. Chris Ashford, ‘Barebacking and the ‘Cult of Violence’: Queering the Criminal Law’ (2010) 74 The Journal of Criminal Law 339, 343. [↑](#footnote-ref-81)
82. For the distinction, see C. F. Stychin, *A Nation by Rights* (Temple University Press: Philadelphia, 1998) 200. [↑](#footnote-ref-82)
83. It has been said that the effeminate queer man is ‘the perceived impediment to queer male social ascension’ (Lawless (n 37) 3). [↑](#footnote-ref-83)
84. Bartone (n 70) 517. For the theory of social-dominance orientation, see Felicia Pratto and others, ‘Social dominance orientation: A personality variable predicting social and political attitudes’ (1994) 67(4) Journal of Personality and Social Psychology 741, 742. [↑](#footnote-ref-84)
85. John Edward Campbell, *Getting It On Online: Cyberspace, Gay Male Sexuality and Embodied Identity* (New York: Harrington Park, 2004) 68. [↑](#footnote-ref-85)
86. According to Penney (n 60), when ‘enough people together make demands publicly for only gym-fit, white men, or even if all believe that they are entitled to nothing less, difference flees from what is essentially a user-generated fascistic model of participation.’  [↑](#footnote-ref-86)
87. # See, for instance, Isabel Scott et al., ‘Context-dependent preferences for facial dimorphism in a rural Malaysian population’ (2008) 29(4) Evolution and Human Behaviour 289.

    [↑](#footnote-ref-87)
88. 6 per cent of the respondents did not indicate their sexuality. [↑](#footnote-ref-88)
89. 8 per cent of the respondents did not indicate their gender. [↑](#footnote-ref-89)
90. By femme-phobia, we mean a discriminatory or otherwise intolerant behaviour against men whose gender performance is perceived as feminine. [↑](#footnote-ref-90)
91. Internalised homophobia is the often-subconscious adoption of homophobic beliefs and behaviours by non-heterosexual men. [↑](#footnote-ref-91)
92. By queerphobia, we mean a discriminatory or otherwise intolerant behaviour against men whose gender performance is perceived as non-binary or otherwise gender non-conforming. [↑](#footnote-ref-92)
93. Bartone (n 70) 517. [↑](#footnote-ref-93)
94. Lawless (n 37) 2. [↑](#footnote-ref-94)
95. eg Alice Marwick Alice, ‘Gender, Sexuality and Social Media’ in Jeremy Hunsinger and Theresa M. Senft (eds), *The Social Media Handbook* (Abingdon: Routledge 2013) 59; Noémie Marignier, ‘“Gay ou pas gay?” Panique énonciative sur le forum jeuxvideo.com’ (Genre, sexualité & société, 1 June 2017) <gss.revues.org/3964> accessed 31 October 2017. [↑](#footnote-ref-95)
96. One of the internal reviewers pointed out that there are also ‘alternative’ spaces such as Growlr (app designed for the ‘bear’ population), where unfit bodies are sought after. However, this research analysed only the main apps used by the general MSM population, leaving out the apps that target specific subgroups, for which different rules and aesthetic standards may apply. Nonetheless, the critique may be placed in the broader context of those studies that claim that online practices give rise to new expressions of gender and sexuality (see, for instance, Sébastien François, ‘Fanf(r)ictions. Tensions identitaires et relationnellles chez les auteurs de récits de fans’ (2009) 1(153) Réseaux 157; Céline Metton-Gayon, *Les adolescents, leur téléphone et Internet. « Tu viens sur MSN?* » (Paris: L’Harmattan 2009). [↑](#footnote-ref-96)
97. Respondent 262768-262760-23304805, response to the MSM survey. [↑](#footnote-ref-97)
98. Respondent 262768-262760-21618126, *ibid*. [↑](#footnote-ref-98)
99. Respondent 262768-262760-22124066, *ibid*. [↑](#footnote-ref-99)
100. Respondent 262768-262760-22435340, *ibid*. This respondent did not answer the question about the difference between online and offline aesthetic discrimination. However, it is believed that while offline discrimination may be perceived as more violent, the online one may be equally damaging because anonymous and because the online/offline divide does not seem any longer tenable. It has been noted that anonymous, spontaneous, disinhibited, and impersonal nature of online interaction will increase the likelihood that prejudice will be expressed more overtly (Jack Glaser and Kimberly Kahn, 'Prejudice, discrimination, and the Internet' in Y. Amichai-Hamburger (ed), *The Social Net: Understanding Human Behavior in Cyberspace* (Oxford: OUP, 2005) 247). According to Brendesha M. Tynes et al., 'Online Racial Discrimination and Psychological Adjustment Among Adolescents' (2008) 43(6) Journal of Adolescent Health 565, "(c)onsistent with offline studies, online racial discrimination was negatively associated with psychological functioning". More recently, on online-offline dichotomy as problematic see Lina Eklund, 'Bridging the online/offline divide: The example of digital gaming' (2015) 53 Computers in Human Behavior 527. [↑](#footnote-ref-100)
101. Respondent 262768-262760-21641632, response to the MSM survey. [↑](#footnote-ref-101)
102. Respondents 262768-262760-22758557 and 262768-262760-22767053. [↑](#footnote-ref-102)
103. See Aliza Friedman and others, ‘Effects of Weight Stigma Concerns, Perceived Discrimination, and Weight Bias Internalization on Disordered Eating in Bariatric Surgery Patients’ (2015) 39(S1) Canadian Journal of Diabetes S46; Janine B. Beekman and others, ‘Effects of perceived weight discrimination on willingness to adopt unhealthy behaviors: Influence of genomic information’ (2015) 31(3) Psychol Health 334. [↑](#footnote-ref-103)
104. Jessica Strubel and Trent A Petrie, ‘Love me Tinder: Body image and psychosocial functioning among men and women’ (2017) 21 Body Image 34. [↑](#footnote-ref-104)
105. ibid 38. [↑](#footnote-ref-105)
106. In the UK, for instance, the protected characteristics are race, age, sex (including being or becoming a transsexual person), civil status, pregnancy, disability, religion, belief, and sexual orientation (Equality Act 2010, ss 4-12). Therefore, whereas discrimination based on homophobia, ageism and ableism is illegal, fattism, body shaming, slut shaming, queer-phobia, etc. are not. [↑](#footnote-ref-106)
107. Currently, in the UK, discrimination is illegal if carried out at work, in education, as a consumer, when using public services, when buying or renting a property, and as a member or guest of a private club or association. On fattism and employment see Mark V. Roehling, ‘Weight-based discrimination in employment: psychological and legal aspects’ (1999) 52 Pers Psychol 969; more generally see Elizabeth E. Theran, ‘Legal theory on weight discrimination’ in Kelly D. Brownell and others (eds), *Weight Bias: Nature, Consequences, and Remedies* (New York: Guilford, 2005) 195. [↑](#footnote-ref-107)
108. Email of MSM app No 1’s spokesperson to this author, 2 March 2017. For ethical reasons, full anonymity was ensured; therefore the reference will be to MSM app No 1 and No 2. The participants to the survey were not requested to disclose personal data and were associated to a unique code for ease of analysis. [↑](#footnote-ref-108)
109. Martin P. Levine, ‘The Gay Clone’ in Robert A. Nye (ed), *Sexuality* (Oxford: OUP, 1999) 376. [↑](#footnote-ref-109)
110. Penney (n 60). [↑](#footnote-ref-110)
111. One of the internal reviewers raised the point that many MSM apps enable their users to identify as belonging to a tribe (eg ‘twinks’, ‘daddies’, etc.). This may suggest that differences are encouraged. However, the apps provide a predefined architecture of choice *ie* the user needs to identify in one of the pre-designed tribes, they cannot create a new tribe; this does not seem to encourage real diversity. Second, many tribes do not have much to do with the body (eg discreet, geek, jock, leather, poz, rugged). [↑](#footnote-ref-111)
112. Hornet Etiquette Guide, <love.hornetapp.com/etiquette-guide/> accessed 25 September 2017 (the website does not clarify when the guide was last updated). [↑](#footnote-ref-112)
113. Interview of this author to a spokesperson for the MSM app No 2. [↑](#footnote-ref-113)
114. Respondent 262768-262760-21618126, response to the MSM survey. [↑](#footnote-ref-114)
115. Confirming and refuting hypothesis may be seen as quantitative pursuit. What the author intends to say it that the no other participants reported the problem of having the profile pictures suspended because they did not meet certain aesthetical standards. [↑](#footnote-ref-115)
116. Dang (n 33) 19-20. [↑](#footnote-ref-116)
117. It has been noted that ‘*Jack’d* suggests the users to choose whether their body type is ‘bear’ or ‘not bear’, ‘masculine’ or ‘not masculine’, which may lead its users to think ‘bear and masculine is the mainstream body type’’ (*ibid* 20). [↑](#footnote-ref-117)
118. Travel Gay Asia and Gay Star News (n 54). [↑](#footnote-ref-118)
119. The cited study does not specify whether the said abuse and harassment relate to body image. [↑](#footnote-ref-119)
120. Respondent 262768-262760-21617248, response to MSM survey. [↑](#footnote-ref-120)
121. Respondent 262768-262760-21633723 *ibid*. [↑](#footnote-ref-121)
122. Respondent 262768-262760-21641632 *ibid*. [↑](#footnote-ref-122)
123. *ibid*. [↑](#footnote-ref-123)
124. *ibid*. [↑](#footnote-ref-124)
125. *ibid*. [↑](#footnote-ref-125)
126. The idea of dating as a new economic market was presented by Marie Bergström, *Au bonheur des rencontres. Classe, sexualité et rapports de genre dans la production et l’usage des sites de rencontres en France* (Paris: SciencesPo, PhD Dissertation, 2014). [↑](#footnote-ref-126)
127. This is mirrored in the near absence of sexuality-related diversity in the corporate social responsibility policies. *Cf* João Bôsco Góis and Kamila Cristina de Silva Teixeira, ‘Diversity in Corporate Social Responsibility: The (Almost Invisible) Place of Homosexuality’ (2011) 13(S1) Culture Health & Sexuality S130. [↑](#footnote-ref-127)
128. 7Park Data (n 46). [↑](#footnote-ref-128)
129. H Dittmar and S Howard, ‘Thin-ideal internalization and social comparison tendency as moderators of media models’ impact on women’s body-focused anxiety’ (2004) 23 Journal of Social and Clinical Psychology 747. For a contrary opinion, see B Martin, E Veer and S Pervan, ‘Self-referencing and consumer evaluations of larger-sized female models: A weight locus of control perspective’ (2007) 18(3) Marketing Letters 197. [↑](#footnote-ref-129)
130. Respondent 262768-262760-21766224, response to MSM survey. [↑](#footnote-ref-130)
131. This is due to the current restrictions to discrimination laws, that allow a number of discriminatory practices if carried out against categories that the legislators and the courts do not think to deserve protection (eg against obese people or queer individuals). Needless to say, however, that a discriminatory act can qualify as illegal under laws that are not related to discrimination (eg hate speech). [↑](#footnote-ref-131)
132. *Scarlet* (n 4). [↑](#footnote-ref-132)
133. The eCommerce Directive provides partly different rules for the immunities of different providers of an information provider service, namely mere conduit, caching, hosting. In this chapter, the focus will be on hosting because MSM app providers are likely to fall under said regime, if they are not publishers in the first place. [↑](#footnote-ref-133)
134. eCommerce Directive, art 14(1)(a). [↑](#footnote-ref-134)
135. eCommerce Directive, art 14(1)(b). The notice-and-takedown mechanisms have not been harmonised yet.  Some countries have sector specific rules (on terrorism, child porn, etc.), only a few Member States have detailed the timescale of the takedown. Moreover, national courts take different approaches when deciding whether an intermediary has actual knowledge. See Commission, ‘Commission Staff Working Document “Bringing e-commerce benefits to consumers”’ (SEC(2011) 1640 final). [↑](#footnote-ref-135)
136. See *e.g.* Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online (C(20181177 final), para. 8. [↑](#footnote-ref-136)
137. *Herrick* v *Grindr, LLC*, No. 1:2017cv00932 - Document 21 (S.D.N.Y. 2017). [↑](#footnote-ref-137)
138. The US Court of the Southern District of New York denied an application for extension of temporary restraining order (TRO). The parties will appear for an initial pre-trial conference on 10 March 2017.  [↑](#footnote-ref-138)
139. Matthew Herrick (@MatthewSHerrick), tweet of 6 February 2017, 1:14AM <twitter.com/MatthewSHerrick/status/828411528441372672> accessed 28 September 2017. [↑](#footnote-ref-139)
140. See Daniel De Simone, ‘The killer the police missed’ (*BBC* *News*, 25 November 2016) <www.bbc.co.uk/news/resources/idt-d32c5bc9-aa42-49b8-b77c-b258ea2a9205> accessed 25 September 2017. [↑](#footnote-ref-140)
141. cf Graham Gremore, ‘Why is Grindr refusing to cooperate more in the search for this missing grad student?’ (Queerty, 6 March 2017) <www.queerty.com/grindr-refusing-cooperate-search-missing-grad-student-20170306> accessed 25 September 2017. [↑](#footnote-ref-141)
142. One of the internal reviewers underlined that this is a speculative exercise, but other explanations may apply. It may be that Grindr did not have any information that could help the investigations. This may well be, but it would be surprising, given the amount and granularity of data MSM apps collect for a number of reasons, including advertising. [↑](#footnote-ref-142)
143. Defamation Act 1996, s 1 [↑](#footnote-ref-143)
144. Defamation Act 2013, ss 5 and 10. Under s 5 of this Act, the Defamation (Operator of Websites) Regulations 2013 were made. [↑](#footnote-ref-144)
145. According to *Metropolitan International Schools Ltd* v *Designtechnica Corporation, Google UK Ltd & Google Inc* [2009] EWHC 1765 (QB), it does. [↑](#footnote-ref-145)
146. eCommerce Regulations, regs 17-19. [↑](#footnote-ref-146)
147. Intermediaries shall make available the details of the service provider, including their email address, which make it possible to contact them rapidly and communicate with them in a direct and effective manner. [↑](#footnote-ref-147)
148. ## For more information, see Open Rights Group, 'eBay must stop Epson’s patent abuse' (*Open Rights Group*, 25 October 2017) <www.openrightsgroup.org/press/releases/2017/ebay-must-stop-epson-patent-abuse> accessed 25 October 2017.

     [↑](#footnote-ref-148)
149. # For a recent expression of this trend, see, for instance, Michał Sałajczyk, 'Poland: File hosting platform ordered to monitor its resources for pirated films' (*MediaWrites*, 11 October 2017) <www.mediawrites.law/file-hosting-platform-ordered-to-monitor-its-resources-for-pirated-films/> accessed 25 October 2017.

     [↑](#footnote-ref-149)
150. See Centre for Democracy and Technology, 'Intermediary liability: protecting internet platforms for expression and innovation' (*CDT*, April 2010) <www.cdt.org/files/pdfs/CDT-Intermediary per cent20Liability\_(2010).pdf> accessed 24 October 2017. [↑](#footnote-ref-150)
151. In some instances, privacy may be a serious concern, see *CG* v *Facebook Ireland Ltd* [2015] NIQB 11, where Facebook was ordered to pay damages to a convicted sex offender, and to remove a page from its website which had been set up with the purpose of driving sex offenders in Northern Ireland from their homes and exposing them to vilification and the risk of serious harm. The sex offender had had an expectation of privacy in respect of his personal information. See also *J20* v *Facebook Ireland Ltd* [2016] NIQB 98. [↑](#footnote-ref-151)
152. *Scarlet* (n 4). [↑](#footnote-ref-152)
153. *ibid* [50]. [↑](#footnote-ref-153)
154. Lilian Edwards, ‘The Fall and Rise of Intermediary Liability Online’ in Lilian Edwards and Charlotte Waelde, *Law and the Internet* (London: Hart, 3rd ed, 2009) 47, 59. [↑](#footnote-ref-154)
155. Commission, ‘Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms’ (Communication) COM (2017) 555 final, para 3(3)(2). This is consistent with the eCommerce Directive, recital 40, whereby ‘the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.’ [↑](#footnote-ref-155)
156. cf Lilian Edwards, ‘The Role of Internet Intermediaries in Advancing Public Policy Objectives Forging Partnerships for Advancing Policy Objectives for the Internet Economy, Part II’ (*SSRN*, 22 June 2011) <ssrn.com/abstract=1875708> accessed 28 September 2017. [↑](#footnote-ref-156)
157. Lilian Edwards, ‘Should ISPs Be Compelled to Become Copyright Cops? File-Sharing, the Music Industry and Enforcement Online’ (*SSRN*, 16 July 2009) <https://ssrn.com/abstract=1435115> accessed 28 September 2017. [↑](#footnote-ref-157)
158. Felipe Romero-Moreno, ‘The Digital Economy Act 2010: subscriber monitoring and the right to privacy under Article 8 of the ECHR’ (2016) 30(3) International Review of Law, Computers, & Technology 229. [↑](#footnote-ref-158)
159. Internet service providers shall notify their subscribers if their IP address has been reported as associated to copyright infringement. Moreover, they have to monitor the reports and compile an anonymous ‘copyright infringement list’ of those who have received three or more notifications in one year. [↑](#footnote-ref-159)
160. Digital Economy Act 2010, s 3. [↑](#footnote-ref-160)
161. European Convention on Human Rights, art 8. [↑](#footnote-ref-161)
162. Commission, ‘Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms’ (Communication) COM (2017) 555 final, para 1. [↑](#footnote-ref-162)
163. EDiMA, ‘EDiMA strongly disappointed at the European Commission announcements regarding new Platform Regulation initiatives’ (*EDiMA*, 10 May 2017) <http://www.europeandigitalmediaassociation.org/pdfs/latest\_news/Press%20Release%20-%20EDiMA%20Mid-term%20review%20reaction.pdf> accessed 13 November 2017. [↑](#footnote-ref-163)
164. In replying to this communication, it has been underlined that ‘(a)ny regime for tackling illegal content on the internet has to be carefully calibrated to ensure respect for the fundamental rights on which our society and our democracy are based’ (European Digital Rights, ‘Letter to the Digital Economy Commissioner Mariya Gabriel “A coherent and rights-based approach to dealing with illegal content”’ (EDRI, 20 October 2017) <https://edri.org/files/letter\_coherent\_rightsbasedapproach\_illegalcontent\_20171020.pdf> accessed 12 November 2017). This author agrees with the statement according to which ‘not acceptable for governments to encourage or coerce internet intermediaries to take measures “voluntarily” that would not be permitted by international law or national constitutions, if they were provided for by law.’ (ibid 2). [↑](#footnote-ref-164)
165. Charlotte Waelde and Lilian Edwards, ‘Online Intermediaries and Copyright Liability’ (2005) WIPO Workshop Keynote Paper <ssrn.com/abstract=1159640>. [↑](#footnote-ref-165)
166. See, for instance, Office for National Statistics, ‘Crime in England and Wales: year ending May 2017’ (ONS, 20 July 2017) 42 <www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2017> accessed 25 September 2017, which states that ‘(a)dults aged 16 and over experienced an estimated 3.4 million incidents of fraud in the survey year ending March 2017 (…), with over half of these (57 per cent; 1.9 million incidents) being cyber-related.’ [↑](#footnote-ref-166)
167. On the relevance of the active role in finding intermediary liability see, for instance, Case C-324/09 *L’Oréal SA and Others* v *eBay International AG and Others* [2011] ECR I-6011, para 116, where the Court of Justice stated that intermediaries cannot claim immunity under the eCommerce Directive (art. 14(1)), if they "have played an active role of such a kind as to give it knowledge of, or control over, the data" relating to the allegedly illegal activity carried out by the platform's users. [↑](#footnote-ref-167)
168. Whilst discriminatory practices online are not illegal per se (eg if not related to employment, education, etc.), they may become illegal, for instance if they qualify as hate speech. In the event of theft of the profile picture for the creation of fake profiles, then, the platform may be found liable inter alia for copyright infringement (leaving aside criminal law, see The Crown Prosecution Service, ‘Guidelines on prosecuting cases involving communications sent via social media’ (*CPS*, 3 March 2016) <www.cps.gov.uk/legal/a\_to\_c/communications\_sent\_via\_social\_media/> accessed 26 September 2017). [↑](#footnote-ref-168)
169. Grindr Terms and Conditions of Service (hereinafter Grindr Terms), clause 10(4). The text is available at<www.grindr.com/terms-of-service> accessed 25 September 2017 (the website does not clarify when the terms were last updated). [↑](#footnote-ref-169)
170. *ibid* clause 10(4). See also clause 12(4). Similar provisions can be found in other platforms; see, for instance, the Hornet Terms of Service (hereinafter Hornet Terms), clause 7(c) <love.hornetapp.com/terms-of-service/> accessed 26 September 2017: ‘Hornet assumes no responsibility whatsoever in connection with or arising from User Submissions (…) reserves the right to prevent you from submitting User Submissions.’ [↑](#footnote-ref-170)
171. Grindr Privacy Policy <www.grindr.com/privacy-policy> accessed 28 September 2017. These data are shared inter alia with the Chinese parent company; one may doubt, however, that the users are aware of this and that the Chinese privacy laws ensure the same level of protection as the European ones, let alone the same level of protection for LGBT rights. See, respectively, Bo Zhao and G. P. (Jeanne) Mifsud Bonnici, ‘Protecting EU citizens’ personal data in China: a reality or a fantasy?’ (2016) 24(2) International Journal of Law and Information Technology 28 and Talha Burki, ‘Health and rights challenges for China's LGBT community’ (2017) 389(10076) The Lancet 1286. Hornet is not clear on the point of which data are collected and with whom they are shared, but the reference to ‘habits, characteristics and user patterns’ may well include private messages (Hornet Privacy Policy < love.hornetapp.com/privacy-policy/> accessed 28 September 2017). Likewise, PlanetRomeo stores the personal data provided when creating an account ‘as well as other Personal Data provided by you when you use the Service.’ (PlanetRomeo Privacy Statement <www.planetromeo.com/en/privacy/> accessed 28 September 2017). [↑](#footnote-ref-171)
172. *ibid*. [↑](#footnote-ref-172)
173. While direct marketing is a legitimate use under the GDPR, recital 47, the consent is still required by the Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426. The draft ePrivacy Regulation (Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC) keeps consent as a requirement for direct marketing (recital 33), save the right to withdraw consent ‘at any time in an easy manner’ (recital 34). See also ePrivacy Regulation, art 16. [↑](#footnote-ref-173)
174. Whilst the profile pictures are subject to an *ex-ante* control, profile descriptions are monitored mostly *ex post*. [↑](#footnote-ref-174)
175. Filtering or human moderation give ‘providers knowledge of a variety of different kinds of illegality’ (Christina Angelopoulos, ‘MTE v Hungary : A new ECtHR judgment on intermediary liability and freedom of expression’ (2016) 11(8) Journal of Intellectual Property Law & Practice 582, 584). [↑](#footnote-ref-175)
176. One of the internal reviewers suggested that this might explain the rejection of fig 1. Arguably, one photo arguably ‘suggests’ nudity, in the other the towel slips ‘suggestively’. [↑](#footnote-ref-176)
177. There is a clear imbalance of power between the app stores (at least those provided by Google and Apple) and the app providers. This may explain the imposition of the very strict legals of the MSM apps, that ban every user-generated content even vaguely inappropriate or even immoral. Apple’s guidelines seem, however, not as strict where they exclude only ‘(o)vertly sexual or pornographic material’ (Apple App Store Review Guidelines, para 1.1.4 <developer.apple.com/app-store/review/guidelines/> accessed 27 September 2017), which is quite different to Hornet’s ban, covering even ‘(p)hotos with only underpants being worn’ (Hornet Usage Guidelines <love.hornetapp.com/usage-guidelines/> accessed 27 September 2017). A middle way, Google does not allow explicit content, such as pornography, and ‘sexually gratifying’ content (Google Play Developer Program Policies, < https://play.google.com/intl/None/about/developer-content-policy-print/> accessed 12 November 2017).

     For a discussion on the vagueness of Apple’s developer guidelines and the uncertainty and opaqueness of its approval process see Luis E. Hestres, ‘App Neutrality: Apple’s App Store and Freedom of Expression Online’ (2013) 7 International Journal of Communication 1265. [↑](#footnote-ref-177)
178. All the MSM apps’ legals refer to the app stores guidelines, but only Grindr expressly incorporates, at the end of its Terms, the ‘Apple Store Additional Terms and Conditions.’ In the Hornet Usage Guidelines, then, one can read that ‘(w)e have to honor some guidelines by our partners Apple and Google, among others. If we don't - bam - Hornet gets pulled quicker than a quick thing on National Quick Day.’ [↑](#footnote-ref-178)
179. State of California Office of the Attorney General (Kamala D. Harris), ‘The Joint Statement of Principle’ (*California Office of Attorney General*, 22 February 2012) <oag.ca.gov/system/files/attachments/press\_releases/n2630\_signed\_agreement.pdf> accessed 27 September 2017. [↑](#footnote-ref-179)
180. Daithí Mac Síthigh ‘App law within: rights and regulation in the smartphone age’ (2013) 21(2) International Journal of Law and Information Technology 154, 179. [↑](#footnote-ref-180)
181. Adrian Fong, ‘The role of app intermediaries in protecting data privacy’ (2017) 25(2) International Journal of Law and Information Technology 85. [↑](#footnote-ref-181)
182. The other spokesperson preferred not to disclose information about how the app store providers ensure that the MSM app providers comply with their content policies. [↑](#footnote-ref-182)
183. There may be different mechanisms to ensure the app providers’ compliance with the app store’s guidelines. For instance, developers that wish that their apps be available on Google Play are required to fill in a questionnaire about the nature of the app’s content and in case of misrepresentation that app may be removed or suspended (Google Play Developer Program Policies, para ‘Content Ratings’). However, it is not clear how Google ensures that the app providers do not make any misrepresentation. [↑](#footnote-ref-183)
184. Síthigh (n 178) 180. [↑](#footnote-ref-184)
185. Interview with spokesperson of MSM app no 1 and no 2. [↑](#footnote-ref-185)
186. App Store Review Guidelines, para 1.1.1. [↑](#footnote-ref-186)
187. While PlanetRomeo Terms of Use (hereinafter PlanetRomeo Terms <www.planetromeo.com/en/terms-of-use/> accessed 27 September 2017) do not provide anything on the point, Grindr makes a generic mention to ‘racially or ethnically or otherwise offensive’ content (Grindr Terms clause 8(3)(12)) and Hornet to ‘racially or ethnically offensive’ content (Hornet Terms, clause 5(i). [↑](#footnote-ref-187)
188. App Store Review Guidelines, para 1.2. Google Play Store’s guidelines are not explicit on the point, but they state that ‘(a)pps that contain or feature user-generated content (UGC) must take additional precautions in order to provide a policy compliant app experience.’ (Developer Program Policies, para ‘User Generated Content’). [↑](#footnote-ref-188)
189. Grindr Terms, clause 18(1). Similarly, see Hornet Terms, clause 13(4). [↑](#footnote-ref-189)
190. PlanetRomeo Terms, clause 10(4). [↑](#footnote-ref-190)
191. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ 178. The withdrawal of the UK from the EU is unlikely to directly affect the regimes introduced as a consequence of EU Directives, because they were transposed into national legislation. However, after the completion of the leaving process, the UK will be free to introduce diverging eCommerce legislation and case law. [↑](#footnote-ref-191)
192. Electronic Commerce (EC Directive) Regulations 2002, SI 2001/2555 (eCommerce Regulations); see, in particular, regs 17-19. [↑](#footnote-ref-192)
193. Under the eCommerce Directive, for instance, ‘(i)n order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned’ (recital 46). [↑](#footnote-ref-193)
194. ‘The User's only remedy in the event of an attributable failure or unlawful acts of PlanetRomeo, is to discontinue the use of the Service’ (Romeo Terms, 10(2)). [↑](#footnote-ref-194)
195. *Scarlet* (n 4). [↑](#footnote-ref-195)
196. In countries where homosexuality is stigmatised or criminalised, MSM apps may send the users a warning, but it ‘is questionable whether such a built in feature can be demanded from the provider of the app’ (Lodder (n 34) 12). [↑](#footnote-ref-196)
197. Commission, ‘Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms’ (Communication) COM (2017) 555 final, para 1. [↑](#footnote-ref-197)
198. *Delfi AS*v*Estonia* [GC], no. 64569/09 [2015] ECHR [159]. [↑](#footnote-ref-198)
199. At the European level, see the Data Protection Directive, the GDPR, and the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002) OJ L 201). In the UK, see, mainly, the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426. See also the Data Protection HL Bill (2017-19) 66. Introduced in September 2017 to implement the GDPR, it is currently at the committee stage at the House of Lords. [↑](#footnote-ref-199)
200. The principle of technological neutrality, whereby laws should not deal with specific technologies, is only a partial solution to the problem. First, there are several exceptions to the principle. For instance, under Article 8(1) of the Vienna Convention on Road Traffic, ‘(e)very moving vehicle or combination of vehicles shall have a driver.’ Therefore, currently if a party to this convention authorised driverless cars on its territory, they would be in breach of their international obligations. See Hans-Heinrich Trute, ‘The Internet of Things: Remarks from the German Perspective’ (2016) 5 Journal of Law & Economic Regulation 118, 135). More generally, even when the law does not target a specific technology, it is adopted with a specific technological context in mind. An example may be copyright law, which was designed for a world of books and photocopies and, therefore, struggles in an era of Snapchat selfies and cloud storage. Ysolde Gendreau, ‘A Technologically Neutral Solution for the Internet: Is It Wishful Thinking?’ in Joost Blom and Hélène Dumont (eds), Science, Truth and Justice (Canadian Institute for the. Administration of Justice, Themis, 2000) 199, 214 notes that what ‘may today be considered technologically neutral may at a later date be viewed as technologically specific.’ She believes that the solution could be found in favouring ‘general principles over arcane technicalities’ (ibid 214-215), in other terms a ‘*droit d’auteur’* approach over a copyright one. Cf, more recently, Kelvin Sum, ‘Syncing copyright with the online digital environment’ (SLS 2017 conference, 8 September 2017, Dublin). [↑](#footnote-ref-200)
201. By private ordering, traditionally, one means the delegation of regulatory powers to private actors (the ICANN being the classic example). However, here by private ordering it is meant the *de-facto* delegation of the regulation of the online environment to contractual and quasi-contractual agreements that fill the gaps left by traditional regulation and legislation, that often is already old in the moment when it is adopted. On the traditional concept, see Steven L. Schwarcz, ‘Private ordering’ (2002) 97(1) Northwestern University Law Review 319. For a range of possible meanings of ‘private ordering’ see David Castle (ed.), *The Role of Intellectual Property Rights in Biotechnology Innovation* (Cheltenham: Elgar, 2009) 312 fn 42-44. [↑](#footnote-ref-201)
202. For a deeper analysis of online private ordering, see Guido Noto La Diega and Ian Walden, ‘Contracting for the ‘Internet of Things’: Looking into the Nest’ (2016) 2 European Journal of Law & Technology 1. On the importance of plain and legible terms see Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29, recital 20, arts 4(2) and 5; Case C‑26/13 *Árpád Kásler and Hajnalka Káslerné Rábai* v *OTP Jelzálogbank Zrt* [2014] ECR, paras 60-75. [↑](#footnote-ref-202)
203. Omri Ben-Shahar and Lior Jacob Strahilevitz, ‘Contracting over Privacy: Introduction’ (2016) 45(S2) J Legal Studies S1. [↑](#footnote-ref-203)
204. Yoan Hermstrüwer, ‘Contracting Around Privacy The (Behavioral) Law and Economics of Consent and Big Data’ (2017) 8(1) JIPITEC 9, 17, referring to Omri Ben-Shahar and Carl E. Schneider, ‘The Failure of Mandated Disclosure’ (2011) 159 University of Pennsylvania Law Review 647. [↑](#footnote-ref-204)
205. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (1993) OJ L 95/29, art 4. Similarly, in the UK, the Unfair Terms in Consumer Contracts Regulations 1994, SI 1994/3159, reg 3. [↑](#footnote-ref-205)
206. This is consistent with the existing literature. For instance, it is deemed well-established that ‘readership of terms and conditions, privacy notices, end-user licence agreements and other click-through agreements is generally low’ (Maartje Elshout and others, ‘Study on consumers’ attitudes towards online Terms and Conditions (T&Cs)’ (*European Commission*, 21 March 2016) 9 <ec.europa.eu/consumers/consumer\_evidence/behavioural\_research/docs/terms\_and\_conditions\_final\_report\_en.pdf> accessed 26 September 2017). See also Stuart Moran, Ewa Luger, and Tom Rodden, ‘Literatin: Beyond Awareness of Readability in Terms and Conditions’ (Ubicomp ’14 Adjunct, Seattle, September 2014), who suggest to solve to problem with a Chrome extension that compares the complexity of popular fictional literature to the legals in order to sensitise people to their complexity. See also Ewa Luger, Stuart Moran, and Tom Rodden, ‘Consent for All: Revealing the Hidden Complexity of Terms and Conditions’ (CHI 2013: Changing Perspectives, Paris, April-May 2013). [↑](#footnote-ref-206)
207. Joel R. Reidenberg and others, ‘Ambiguity in Privacy Policies and the Impact of Regulation’ (2016) 45(S2) J Legal Studies S163. [↑](#footnote-ref-207)
208. Respondent 262768-262760-21618126, response to the MSM survey. [↑](#footnote-ref-208)
209. Lior Jacob Strahilevitz and Matthew B. Kugler, ‘Is Privacy Policy Language Irrelevant to Consumers?’ (2016) 45(S2) J Legal Studies S69. [↑](#footnote-ref-209)
210. Elshout (n 204) 10. [↑](#footnote-ref-210)
211. Respondent 262768-262760-21618126, *ibid*. [↑](#footnote-ref-211)
212. Guido Noto La Diega, ‘Uber law and awareness by design. An empirical study on online platforms and dehumanised negotiations’ (2016) 2 European Journal of Consumer Law 383, 410, defines ‘awareness by design’ as ‘the use of technologies (especially design) to empower the user and make them aware of risks, rights, and obligations.’ He makes the example of the replacement of the usual pre-ticked box (‘I have read/I have understood’) boxes with a box whose default option is ‘I have not read/I have not understood.’ [↑](#footnote-ref-212)
213. GDPR, art 25. [↑](#footnote-ref-213)
214. Gamifying privacy seems pivotal to making users take privacy seriously. Indeed, given the tendency not to read the privacy policies, gamification can lead to increased interactivity and thus alertness. See, for instance, Centre for Democracy and Technology ‘The Gamification of Privacy’ (*CDT*, 11 July 2011) <cdt.org/blog/the-gamification-of-privacy/>. Some authors distinguish between serious games and gamified interactions (Cristina Rottondi and Giacomo Verticale, ‘A Privacy-Friendly Gaming Framework in Smart Electricity and Water Grids’ (2017) 5 IEEE Access 14221). The former refers to games designed for purposes others than entertainment, the latter to ‘the use of game design elements in non-game contexts’. In this chapter, it is believed that using game design elements in the drafting and presentation of privacv policies can be a good way to increase the users’ awareness thus making it more likely that they will have privacy-preserving behaviours. Unlike that study, this author is more concerned with the use of games to protect privacy, rather than with the privacy risks of online gaming. [↑](#footnote-ref-214)
215. Competition & Markets Authority, ‘The commercial use of consumer data. Report on the CMA’s call for information’ (*GovUK,* June 2015) 130 <www.gov.uk/government/uploads/system/uploads/attachment\_data/file/435817/The\_commercial\_use\_of\_consumer\_data.pdf> accessed 25 September 2017. [↑](#footnote-ref-215)
216. Certainly, the belief of not having any other choice but accepting the legals plays an important in making users give away their rights. [↑](#footnote-ref-216)
217. The software used was Readable.io. [↑](#footnote-ref-217)
218. ### The Flesch-Kincaid Grade Level rates texts on a US school grade level. For instance, a score of 8.0 means that an eighth grader (Year 9 in England) can understand the document. For most documents, the desirable score is between 7.0 and 8.0. The parameters of this test are word length and sentence length. Cf Glenda M. McClure, ‘[Readability formulas: Useful or useless?](http://ieeexplore.ieee.org/document/6449109/)’ (1987) PC30(1) IEEE Transactions on Professional Communication 12.

     [↑](#footnote-ref-218)
219. The parameters of this test are sentence length and hard words (words with more than two syllables). The desirable score is 8 and it should never go beyond 12 (High School senior). For more details, see Robert Gunning, *The technique of clear writing* (New York: McGraw-Hill, 1952). [↑](#footnote-ref-219)
220. Unlike the two tests above, the Colemain-Liau Index considers the length of the words with regards to the letters, not to the syllables. It looks at the average number of letters and the average number of sentences per 100 words. Like the other tests, the scores approximate the US levels. Therefore, the desirable score is between 7 and 8. For more information, see Meri Coleman and T.L. Liau, ‘A Computer Readability Formula Designed for Machine Scoring’ (1975) 60(2) Journal of Applied Psychology 283. [↑](#footnote-ref-220)
221. This test looks at the words of three or more syllables in three 10-sentence samples. Grades 13-16 require college education, 17-18 graduate training, and 19 and above, higher professional qualification. According to

     Paul Fitzsimmons and others, ‘A readability assessment of online Parkinson's disease information’ (2010) 40 J R Coll Physicians Edinb 292, the SMOG index is better than the Flesch-Kincaid test because the latter would underestimate reading difficulties. For more information, see G. Harry Mc Laughlin, ‘SMOG Grading – A new readability formula’ (1969) May Journal of reading 639. [↑](#footnote-ref-221)
222. This index looks at characters (relevant only here and in the Coleman–Liau Index), words, and sentences. Like most of the tests, it approximates the US grade level. A score of 8 means that a seventh grader would be able to understand the document. The desirable score would be between 8 and 9. See E.A. Smith and R.J. Senter, ‘Automated Readability Index’ (US Defense Technical Information Center, November 1967) <www.dtic.mil/dtic/tr/fulltext/u2/667273.pdf> accessed 29 September 2017. [↑](#footnote-ref-222)
223. The Flesch-Kincaid Reading Ease rates texts on a 100-point scale. The higher the score, the easier it is to understand the document. The desirable score is between 60 and 70 (8th-9th grade, plain English, easily understood by 13- to 14-year-old students). The parameters of this test are word length and sentence length. For more details, see <support.office.com/en-gb/article/Test-your-document-s-readability-85b4969e-e80a-4777-8dd3-f7fc3c8b3fd2#\_\_toc342546557> accessed 29 September 2017. [↑](#footnote-ref-223)
224. This formula looks at the average sentence length and the percentage of unique unfamiliar words. It was designed for children up to the fourth grade. See George Spache, ‘A new readability formula for primary-grade reading materials’ (1952) 53(7) The Elementary School Journal 410. [↑](#footnote-ref-224)
225. This formula focuses on words, difficult words and sentences. Words are difficult if US fourth graders are not familiar with them. It is suitable for children not beyond the 9th grade. See Jeanne S. Chall and Edgar Dale, *Readability Revisited: The New Dale-Chall Readability Formula* (Brookline: Brookline Books, 1995). [↑](#footnote-ref-225)
226. Grindr Terms, clause 5. [↑](#footnote-ref-226)
227. *ibid* clause 8(1). [↑](#footnote-ref-227)
228. Aaron Smith, ‘15% of American adults have used online dating sites or mobile dating apps’ (Pew Research Centre, 11 February 2016) <http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/02/PI\_2016.02.11\_Online-Dating\_FINAL.pdf> accessed 14 November 2017. [↑](#footnote-ref-228)
229. cf Chun-Ying Chen, Susan Pedersen and Karen L. Murphy, ‘Learners' perceived information overload in online learning via computer-mediated communication’ (2011) 19(2) Research in Learning Technology 101. [↑](#footnote-ref-229)
230. For instance, if one uses the calculator available at <www.readabilityformulas.com/dalechallformula/spache-formula.php> accessed 29 September 2017, as opposed to the one provided by Readable.io, one finds that Grindr Terms score 20. [↑](#footnote-ref-230)
231. Using Dale-Chall calculators different to the one provided by Readable.io, the results are different (even though not as much as the one regarding the Spache Formula. For instance, Grindr Terms score 8.2 using the calculator available at <www.readabilityformulas.com/dalechallformula/dale-chall-formula.php> accessed 29 September 2017. [↑](#footnote-ref-231)
232. Eg ‘*Databankenwet*’ and ‘*toerekenbare tekortkoming*’, referring to, respectively, the Dutch Database Act and the liability for attributably failing to perform the agreement. [↑](#footnote-ref-232)
233. See, for instance, Hornet Terms, clause 4, according to which ‘Hornet reserves the right to change, modify, add, or remove portions of this Agreement or any guidelines at any time with or without notice. Your continued use of the Hornet Services after the posting of any modifications or changes constitutes your binding acceptance of such changes’. See also Grindr Terms, clause 8(1). [↑](#footnote-ref-233)
234. The 21 versions of Google’s Privacy Policy are available at <www.google.com/policies/privacy/archive/> accessed 29 September 2017. [↑](#footnote-ref-234)
235. Elshout (n 204). [↑](#footnote-ref-235)
236. Under the PlanetRomeo Terms of Use, ‘(t)he use of the Service may not (…) involve any illegal activities or activities that are contrary to morality or public order’ (clause 2(4(j)). Likewise, under Grindr Terms ‘You will NOT post, store, send, transmit, or disseminate any information or material which a reasonable person could deem to be objectionable…, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful’ (clause 8(12). [↑](#footnote-ref-236)
237. In the US, privacy policies can be enforced by the Federal Trade Commission as promises to consumers under the Federal Trade Commission Act, 15 U.S.C. § 45(a), s 5 on unfair methods of competition and unfair or deceptive acts or practices. See Gautam S Hans, ‘Privacy policies, terms of service, and FTC enforcement: broadening unfairness regulation for a new era’ (2012) 19(1) Michigan Telecommunications and Technology Law Review 163. In Europe, the ‘legals’ may be found unenforceable under consumer legislation or sectoral one (see, for instance, *Spreadex Ltd v Cochrane* [(2012) Times, 24 August](https://www.lexisnexis.com/uk/lexispsl/commercial/document/391295/56FC-GDH1-F185-W25B-00000-00/linkHandler.faces?psldocinfo=Spreadex_Ltd_v_Cochrane&A=0.34188658856809506&bct=A&service=citation&risb=&langcountry=GB&linkInfo=F%23GB%23Times%23vol%2508%25sel1%252012%25page%2524%25year%252012%25sel2%2508%25&ps=subtopic%2CCOMMERCIAL%2CNEWSANALYSIS%2C96133%2C155668%2C), [2012] EWHC 1290 (Comm)). [↑](#footnote-ref-237)
238. With regards to massively multiplayer online games (MMO games), Megan Rae Blakely, ‘Subject to Terms and Conditions: User Concepts of Ownership and Intellectual Property in MMOs’ (SLS2017 conference, Dublin, September 2017), found that the relevant legals are not enforced. [↑](#footnote-ref-238)
239. Opaque legals hardly deliver GDPR-compliant consent. More generally, the distinction between form and substance is blurred in the data protection field. [↑](#footnote-ref-239)
240. *Forbrukerrådet* (n 47). [↑](#footnote-ref-240)
241. Screen shown to Grindr’s users after uploading a profile picture. Screenshot taken from an Android device accessed on 7 April 2018 at 17:47 GMT. [↑](#footnote-ref-241)
242. [2010] EWHC 690 (QB). [↑](#footnote-ref-242)
243. *Davison v Habeeb* [2011] EWHC 3031 (QB)applied *Metropolitan International Schools* (n 143), and, therefore, did not held Google liable for their search services, despite their listings and snippets including defamatory content. The reason for that was that ‘the operation of the Google search engine is entirely automatic’ (*Davison* [40]). [↑](#footnote-ref-243)
244. Interview to MSM spokesperson No 1, who said that ‘there is usually a human being, but not for fake profiles. All the pictures are ‘voted’ as non-sexual, illegal, a little bit sexual, etc.’ The spokesperson of the MSM app No. 2 did not know if the screening was human or not. However, on 26 April 2018, the customer support of said spokesperson’s company confirmed that they ‘have a team of dedicated staff members who reviews and double-checks all profile pictures and profile descriptions.’ [↑](#footnote-ref-244)
245. As one can read in *Herrick* (n 135), Grindr’s website stated ‘we have a system of digital and human screening tools to protect our users.’ Such assertion is no longer present. Grindr’s customer support observed that they have a ‘Review Team conducted by humans that review the content of Grindr profiles.’ (B. – Grindr Customer Support, email of 26 April 2018). However, they did not answer this researcher’s question whether ‘the review of the profile pictures and profile descriptions is automated, semi-automated, or entirely human.’ (Email to Grindr Customer Support of 26 April 2018). PlanetRomeo’s customer support pointed out that only profile pictures are reviewed manually, whereas the rest ‘on demand manually and partly automatically’ (S. – PlanetRomeo Customer Support, email of 2 May 2018). [↑](#footnote-ref-245)
246. Screen shown to PlanetRomeo’s users after uploading a picture. Screenshot taken from an Android device accessed on 30 March 2017 at 17:05 GMT. [↑](#footnote-ref-246)
247. Grindr Privacy Policy. [↑](#footnote-ref-247)
248. GDPR, art 5. [↑](#footnote-ref-248)
249. To put it in legalese, ‘for the period necessary to fulfill the purposes outlined in this Privacy Policy, *unless a longer retention period is* *required for the operation of the Grindr Services* *or permitted by law’* (Grindr Privacy Policy, italics added). Since the purposes are not clearly outlines, the retention risks being indefinite. Different terms apply to some jurisdictions. The only special terms that provide a limit to the data retention are the Brazilian Grindr Terms: ‘We will keep the application logs under confidentiality, in a controlled and safe environment, for six (6) months’ (Grindr Special Terms for International Users, 8(5)). The special terms are available below the regular terms. [↑](#footnote-ref-249)
250. GDPR, art 89. It should be kept in mind, however, that further processing may be lawful also outside said exception, if personal data is processed in a manner that is compatible with the original purposes (GDPR, art 5(1)(b)). [↑](#footnote-ref-250)
251. GDPR, art 89(1). [↑](#footnote-ref-251)
252. On 8 April 2018, this author reiterated the request. As of 4 May 2018, Grindr has not followed up on the data subject request. [↑](#footnote-ref-252)
253. Consent is not the only legal basis for processing. From the outset, one should assess if Grindr may rely on the necessity for the performance of a contract or on the legitimate interest of the data controller (GDPR, art 6(1)(b) and (f)). It is implausible that the sharing of personal data including sexual data and health data with advertisers and other third parties is necessary for the performance of the contract. This justification may cover, conversely, the processing of geolocation data, since the purpose of the service is to enable users to get in contact with other users based on the respective location. It is unlikely, then, that the company can avail itself of the legitimate interest justification because in light of the type of data processed, the processing should be regarded as very intrusive. Moreover, the MSM survey and the reaction to the HIV status data’s leak confirm that data is not used ‘in ways (data subjects) would reasonably expect’ (Information Commissioner’s Office, *Guide to the General Data Protection Regulation (GDPR)* (v. 1.0.17, ICO 2018) 40. For a recent failure of the legitimate interest defence for availability of less instrusive alternatives see **Commission Nationale de l'Informatique et des Libertés (CNIL), *Décision MED n° 2018- 007 du 5 mars 2018 mettant en demeure la société Direct Energie*.** [↑](#footnote-ref-253)
254. GDPR, arts 4(11) and 7; recitals 32, 33, 42, and 43. See Information Commissioner’s Office (n 25) 20. [↑](#footnote-ref-254)
255. Article 29 Working Party, ‘Guidelines on Consent under Regulation 2016/679’ (WP259, 28 November 2017) 4. [↑](#footnote-ref-255)
256. Grindr Privacy Policy. [↑](#footnote-ref-256)
257. Consent is not freely given, for instance, if ‘the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment’ (GDPR, recital 42). [↑](#footnote-ref-257)
258. Article 29 Working Party (n 253) 19. They suggest also a two-stage verification process, where the data controller informs of the intent of processing sensitive personal data explaining the purposes and the data subject is required to reply ‘I agree.’ [↑](#footnote-ref-258)
259. GDPR, recital 43. [↑](#footnote-ref-259)
260. GDPR, recital 32. [↑](#footnote-ref-260)
261. *ibid.* Screen shown to Grindr’s users after registering but before accessing the service. The screenshot was taken on 4 April 2018 at 16:32 GMT with an Android device. [↑](#footnote-ref-261)
262. *Cf.* Article 29 Working Party (n 253) 14. [↑](#footnote-ref-262)
263. For the requirement of informed consent, see Article 29 Working Party (n 253) 13. [↑](#footnote-ref-263)
264. Article 29 Working Party (n 253) 18. Even though the GDPR does not expressly require prior consent, this is implied in art 6 and recital 40. [↑](#footnote-ref-264)
265. First screen shown to Grindr’s new users before accessing the service. The screenshot was taken on 4 April 2018 at 16:23 GMT with an Android device. [↑](#footnote-ref-265)
266. Article 29 Working Party (n 253) 6. This is in line with the GDPR, art 7(4). [↑](#footnote-ref-266)
267. GDPR, art 7(4). The Article 29 Working Party makes the example of photo editing app collecting geolocation data for behavioural advertising purposes. Since this goes beyond what is necessary for the provision of the service and since ‘users cannot use the app without consent (…) consent cannot be considered as being freely given.’ (*ibid.* 7). [↑](#footnote-ref-267)
268. Grindr Privacy Policy. [↑](#footnote-ref-268)
269. *ibid.*. [↑](#footnote-ref-269)
270. GDPR, art 7(3). [↑](#footnote-ref-270)
271. Article 29 Working Party (n 253) 21. [↑](#footnote-ref-271)
272. The sharing of sensitive personal data for advertising purposes is not unprecedented. For instance, Facebook was fined €1.2 million in Spain for this reason. José González Cabañas, Ángel Cuevas, Rubén Cuevas, ‘Facebook Use of Sensitive Data for Advertising in Europe’ (*ArXiv*, 14 February 2018) <arxiv.org/abs/1802.05030> accessed 18 April 2018 found that Facebook labelled 73% of EU users in association to sensitive personal data. The authors developed a browser extension that Facebook users can use to discover how the social networking site is monetising their data. The tool is available at <fdvt.org/> accessed 18 April 2018. [↑](#footnote-ref-272)
273. Grindr Privacy Policy. [↑](#footnote-ref-273)
274. *Forbrukerrådet* (n 47) 4. [↑](#footnote-ref-274)
275. <www.privacyshield.gov/list> accessed 5 April 2018. The main legal bases for the international data transfers are adequacy decisions, bespoke arrangements, Standard Contractual Clauses, and Binding Corporate Rules. To the knowledge of this author, none of these legal bases applies to the Grindr’s scenario. [↑](#footnote-ref-275)
276. GDPR, art 3(2). [↑](#footnote-ref-276)
277. The evidence of this is the experiment reported in SVT and SINTEF, ‘Grindr Privacy Leaks’ (*GitHub*, 2018) <github.com/SINTEF-9012/grindr-privacy-leaks> accessed 4 May 2018. [↑](#footnote-ref-277)
278. Grindr Privacy Policy. Grindr’s CTO, however, ensures that at least the transmission of HIV status data is encrypted. Scott Chen, ‘Here’s what you should know regarding your HIV status data’ (*Grindr Tumblr*, 3 April 2018) <grindr.tumblr.com/post/172528912083/heres-what-you-should-know-regarding-your-hiv> accessed 6 April 2018. [↑](#footnote-ref-278)
279. GDPR, recital 83. [↑](#footnote-ref-279)
280. GDPR, art 32. [↑](#footnote-ref-280)
281. *Forbrukerrådet* (n 47) 5. [↑](#footnote-ref-281)
282. Article 29 Working Party (n 253) para. 3.3.2. [↑](#footnote-ref-282)
283. See, for instance, Brian Moylan, ‘Grindr was a safe space for gay men. Its HIV status leak betrayed us’ (*The Guardian*, 4 April 2018) <www.theguardian.com/commentisfree/2018/apr/04/grindr-gay-men-hiv-status-leak-app> accessed 4 April 2018. [↑](#footnote-ref-283)
284. Kristine Phillips, ‘Grindr says it will stop sharing users’ HIV data with third-party firms amid backlash’ (*The Washington Post*, 3 April 2018) < www.washingtonpost.com/news/to-your-health/wp/2018/04/03/grindr-says-it-will-stop-sharing-users-hiv-data-with-third-party-firms-amid-backlash/?utm\_term=.a3beb24b874d> accessed 4 April 2018. [↑](#footnote-ref-284)
285. See the Grindr Privacy Policy and Chen (n 276). [↑](#footnote-ref-285)
286. GDPR, art 9(2)(e). [↑](#footnote-ref-286)
287. It has been argued, however, that MSM apps refigure conceptualisations of public/private boundaries. Sam Miles, ‘Sex in the digital city: location-based dating apps and queer urban life’ (2017) 24(11) Gender, Place & Culture 1595/ [↑](#footnote-ref-287)
288. Chen (n 276). [↑](#footnote-ref-288)
289. *ibid.*. [↑](#footnote-ref-289)
290. Grindr Privacy Policy. In the app, it was found the code signature of the following trackers: [AdColony](https://reports.exodus-privacy.eu.org/trackers/90/), [AppsFlyer](https://reports.exodus-privacy.eu.org/trackers/12/), [Apptimize](https://reports.exodus-privacy.eu.org/trackers/135/), [Braze](https://reports.exodus-privacy.eu.org/trackers/17/), [Facebook Ads](https://reports.exodus-privacy.eu.org/trackers/65/), [Facebook Login](https://reports.exodus-privacy.eu.org/trackers/67/), [Facebook Share](https://reports.exodus-privacy.eu.org/trackers/70/), [Google Ads](https://reports.exodus-privacy.eu.org/trackers/71/)

     [Google CrashLytics](https://reports.exodus-privacy.eu.org/trackers/27/), [Google DoubleClick](https://reports.exodus-privacy.eu.org/trackers/5/), [Google Firebase Analytics](https://reports.exodus-privacy.eu.org/trackers/49/), [Inmobi](https://reports.exodus-privacy.eu.org/trackers/106/), [Localytics](https://reports.exodus-privacy.eu.org/trackers/16/), [Millennial Media](https://reports.exodus-privacy.eu.org/trackers/107/), [Moat](https://reports.exodus-privacy.eu.org/trackers/61/), [Smaato](https://reports.exodus-privacy.eu.org/trackers/83/), [Twitter MoPub](https://reports.exodus-privacy.eu.org/trackers/35/). See ‘Grindr – Gay chat, meet & date’ (*Exodus*, 26 March 2018) <reports.exodus-privacy.eu.org/reports/5323/> accessed 4 May 2018. [↑](#footnote-ref-290)
291. This would seem excluded by SVT (n 275). According to said report, Grindr shares with third parties the following data: Grindr (app name), precise GPS position, gender, HIV status, ‘last tested’ date, email address, age, height, weight, body type, position (sexual), Grindr profile ID, ‘tribe’ (Bear, Clean Cut, Daddy, Discreet, Geek, Jock, Leather, Otter, Poz, Rugged, Trans, Unknown), ‘Looking for’ (Chat, Dates, Friends, Networking, Relationship, Right Now, Unknown), ethnicity, relationship status, phone ID, advertising ID, phone characteristics, language, activity. [↑](#footnote-ref-291)
292. Web Foundation, ‘Three challenges for the web, according to its inventor’ (*WebFoundation*, 12 March 2017) <[webfoundation.org/2017/03/web-turns-28-letter/](https://webfoundation.org/2017/03/web-turns-28-letter/)> accessed 19 September 2017. [↑](#footnote-ref-292)
293. Elshout (n 204). [↑](#footnote-ref-293)
294. On the relation between privacy, trust, and purchasing behaviour see Carlos Flavian and Miguel Guinaliu, ‘Consumer trust, perceived security and privacy policy’ (2006) 106(5) Industrial Management & Data Systems 601. [↑](#footnote-ref-294)
295. See, for instance, David Hoffman, ‘Privacy is a business opportunity’ (Harvard Business Review, 18 April 2014) <hbr.org/2014/04/privacy-is-a-business-opportunity> accessed 26 September 2017 and Sören Preibusch, Dorothea Kübler, and Alastair R. Beresford, ‘Price versus privacy: An experiment into the competitive advantage of collecting less personal information’ (2013) 13(4) Electronic Commerce Research 42. It has been pointed out that two solutions to the lack of bargaining power of users of online platforms may be to develop efforts to incentivise service providers to adopt consumer-friendly legals and to raise the awareness of users with regard to the content thereof (Ellen Wauters, Eva Lievens and Peggy Valcke, ‘Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites’ (2014) 22(3) Int J Law Info Tech 254, 293). [↑](#footnote-ref-295)
296. GDPR, art 25. [↑](#footnote-ref-296)
297. GDPR, art 5(2). [↑](#footnote-ref-297)
298. GDPR, arts 5(1)(a) and 12. [↑](#footnote-ref-298)
299. Commission, ‘Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms’ (Communication) COM (2017) 555 final, para 4(2). [↑](#footnote-ref-299)
300. GDPR, art 12, recital 58. [↑](#footnote-ref-300)
301. Allucquère Rosanne Stone, *The War of Desire and Technology at the Close of the Mechanical Age* (Cambridge: MIT Press, 1995) 181 [↑](#footnote-ref-301)
302. Jouët Josiane, ‘Une communauté télématique : les axiens’ (1989) 7(38) Réseaux 49. [↑](#footnote-ref-302)
303. Claire Balleys, ‘L’incontrôlable besoin de contrôle. Les performances de la féminité par les adolescents sur YouTube’ (*Genre, sexualité & société*, 1 June 2017) <gss.revues.org/3958> accessed 31 October 2017. [↑](#footnote-ref-303)
304. Rebecca M. Puhl, Tatiana Andreyeva and Kelly D. Brownell, ‘Perceptions of weight discrimination: prevalence and comparison to race and gender discrimination in America’ (2008) 32 International Journal of Obesity 992, 999. [↑](#footnote-ref-304)
305. The theory was first presented by Kimberle Crenshaw, ‘Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics’ (1989) 1(8) University of Chicago Legal Forum 139. She believed that ‘theories and strategies purporting to reflect the Black community's needs must include an analysis of sexism and patriarchy. Similarly, feminism must include an analysis of race if it hopes to express the aspirations of non-white women’ (*ibid* 166). A more updated idea of intersectionality is presented by Patricia Hill Collins and Sirma Bilge, *Intersectionality* (Polity 2016) 2, according to whom ‘people’s lives and the organization of power in a given society are better understood as being shaped not by a single axis of social division, be it race or gender or class, but my many axes that work together and influence each other.’ Intersectionality evolved to encompass other identities and protected characteristics; see Devon W Carbado, ‘Intersectionality. Mapping the Movements of a Theory’ (2013) 10(2) Du Bois Review 303. For an application related to queer people and Islam see, for instance, Fatima El-Tayeb, ‘’Gays who cannot properly be gay’: Queer Muslims in the neoliberal European city’ (2012) 19(1) European Journal of Women’s Studies 79. [↑](#footnote-ref-305)
306. For instance, racial discrimination is associated with increased body mass index (Gilbert C. Gee and others, ‘Disentangling the effects of racial and weight discrimination on Body Mass Index and obesity among Asian Americans’ (2008) 98(3) American Journal of Public Health 493. [↑](#footnote-ref-306)
307. cf Paul Michaels, ‘The use of dating apps within a sample of the international deaf gay male community’ (IGALA9 conference, Hong Kong, May 206). [↑](#footnote-ref-307)
308. Suffice to say that the first law of usability - *ie* the rules on how a website should be designed – can be summed up as ‘don’t make me think’. If the brain is switched off, it is unlikely the user will behave in a privacy-aware way. See Steve Krug, *Don't Make Me Think: A Common Sense Approach to Web Usability* (San Francisco: New Riders, 2nd ed, 2005). [↑](#footnote-ref-308)
309. Grindr Terms, clauses 2, 8(3)(15) 20. On the enforceability of the most common contractual provisions in online services see Marco Loos and Joasia Luzak, ‘Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers’ (2016) 39 J Consum Policy 63. [↑](#footnote-ref-309)
310. See, for instance, the Consumer Rights Act 2015, s 65. [↑](#footnote-ref-310)
311. Marx, *Capital vol 1* (1867, Chicago: Charles H. Kerr, Eng tr, 1909)291. [↑](#footnote-ref-311)
312. *ibid*. 291. [↑](#footnote-ref-312)
313. When one buys a car, one owns and therefore has exclusive control over the car. If one buys a smart car, one may have control over its hardware, but not on the software and service components. See Myriam Bianco, ‘Take care, Neo: The Fridge has you. A technology-aware legal review of consumer usability issues in the Internet of Things’ (2016) Working paper no 1/2016 <nexa.polito.it/nexacenterfiles/FINAL\_Take%20care,%20Neo\_%20the%20Fridge%20has%20you\_A%20technology-aware%20legal%20review%20of%20consumer%20usability%20issues%20in%20the%20Internet%20of%20Things\_0.pdf > accessed 28 September 2017. There is already case law about preventing owners from using the goods they purchased because of the third parties’ assertion of intellectual property rights (see *MicrobeadsAG* v *Vinhurst Road Markings* [1975] 1 WLR 218). These cases risk becoming commonplace when all the devices embed software or other immaterial goods protected by intellectual property rights. Cf Christopher Millard, W. Kuan Hon and Jatinder Singh, ‘Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities’ (2017) 2017 IEEE International Conference on Cloud Engineering 286, 288; M. Scott Boone, ‘Ubiquituous Computing, Virtual Worlds, and the Displacement of Property Rights’ (2008) 4(1) Journal of Law and Policy 91. [↑](#footnote-ref-313)
314. The circular economy refers to ‘closed production systems, *ie* new systems where resources are reused and kept in a loop of production and usage, allowing to generate more value and for a longer period.’ (Andrea Urbinati, Davide Chiaroni and Vittorio Chiesa, ‘Towards a new taxonomy of circular economy business models’ (2017) 168 Journal of Cleaner Production 487). For the purpose of (with the excuse of) putting in place environmental-friendly policies, the circular economy justifies the retention of the ownership by the manufacturer of the device, who will look after the maintenance and, finally, reuse of the rented / leased device (this idea was suggested by Sean Thomas, ‘Law, the Circular Economy, and Smart Technology’ (SLS2017 conference, Dublin, September 2017). The fact that we no longer own our devices (and more generally goods), however, can have very dangerous consequences (even practical, for instance if a regime like the **Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees** [1994] OJ L 171 does not apply if there is no transfer of ownership). [↑](#footnote-ref-314)
315. For other legal issues of Internet of Things and circular economy, in particular on the competition law implications of the ‘product as a service’ and of the ‘predictive maintenance’, see Marco Ricolfi, ‘IoT and the Ages of Antitrust’ (2017) Nexa Center for Internet & Society Working paper No 4/. [↑](#footnote-ref-315)